Benutzerhandbuch

Ascend Communications

Teile-Nr. 7820-0316-001

FCC Teil 15

Warnung: Dieses Gerät wurde getestet und gemäß den Beschränkungen für ein Digitalgerät der Klasse A in Übereinstimmung mit Teil 15 der FCC-Bestimmungen (Federal Communications Commission, US-amerikanische Bundesbehörde für das Fernmeldewesen) für zulässig befunden. Diese Beschränkungen sollen beim Einsatz des Geräts in einer kommerziellen Umgebung einen angemessenen Schutz gegen schädliche Störungen gewährleisten. Dieses Gerät erzeugt und nutzt Hochfrequenzenergie und kann diese ausstrahlen. Wenn es nicht entsprechend den Anweisungen im Handbuch installiert und eingesetzt wird, kann es Störungen des Funkverkehrs verursachen. Der Betrieb des Geräts in einem Wohngebiet führt sehr wahrscheinlich zu Störungen, die auf Kosten des Betreibers zu beseitigen sind.

Die Genehmigung, dieses Gerät zu betreiben, wird davon abhängig gemacht, daß keine Änderungen am Gerät vorgenommen werden, die nicht ausdrücklich von Ascend genehmigt wurden.

Produktgarantie und Support

Bitte richten Sie Ihre Fragen zur Prodktgarantie und zum Support unserer Geräte an Ihren Händler.

Informationen über neue Leistungsmerkmale und Produkte

Wir arbeiten ständig an der Verbesserung unserer Produkte. Informationen über neue Leistungsmerkmale und Produktverbesserungen erhalten Sie auf den folgenden Wegen:

- Neueste Informationen zu den Ascend-Produkten erhalten Sie unter unserer WWW-Adresse:
  `http://www.ascend.com/`
- Software-Aktualisierungen, Release-Informationen und Zusätze zu diesem Handbuch erhalten Sie unter folgender FTP-Adresse:
  `ftp.ascend.com`

Inhaltsverzeichnis

Abbildungen

Über dieses Handbuch

In diesem Handbuch wird erklärt, wie Sie die Pipeline installieren, konfigurieren und mit ihr arbeiten können. Bei der Arbeit mit der Pipeline sollte dieses Handbuch stets zusammen mit dem *Referenzhandbuch* verwendet werden. Das *Referenzhandbuch* enthält ausführliche Beschreibungen der für die Konfiguration Ihres Gerätes benötigten Parameter.

Aufbau des Handbuchs

Dieses Handbuch enthält die folgenden Kapitel:

- Im Kapitel 1, „Einführung“, finden Sie eine Einführung in die Pipeline sowie Erläuterungen zu einigen der im Zusammenhang mit der Pipeline verwendeten Begriffe.
- Kapitel 2, „Installation der Pipeline“, erläutert, wie Sie die Pipeline installieren.
- Kapitel 3, „Pipeline-Grundeinstellungen“, finden Sie die für die grundlegende Konfiguration Ihrer Pipeline erforderlichen Informationen.
- Im Kapitel 4, „Die Pipeline-Benutzeroberfläche“, wird die Pipeline-Konfigurationsoberfläche beschrieben.
- Im Kapitel 5, „Konfigurieren von WAN-Verbindungen“, wird gezeigt, wie Sie die Pipeline für verschiedene Verbindungsarten mit dem WAN konfigurieren können.
- Im Kapitel 6, „Konfigurieren der Pipeline als Bridge“, wird erklärt, wie Sie die Pipeline für das Bridging konfigurieren können.
- Im Kapitel 7, „Konfigurieren der Pipeline als IP-Router“, wird erklärt, wie Sie die Pipeline für das IP-Routing konfigurieren können.

- Im Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“, wird erklärt, wie Sie die Pipeline für das IPX-Routing konfigurieren können.
- Im Kapitel 9, „Einrichten der Pipeline-Sicherheit“, wie Sie die Pipeline-Sicherheitsmaßnahmen konfigurieren können.
- Im Kapitel 10, „Definieren von Filtern“, wird die Arbeitsweise von Filtern erklärt, und es wird gezeigt, wie Sie Filter definieren können.
- Im Kapitel 11, „Systemadministration“, wird erklärt, was bei der Pipeline-Administraton zu beachten ist.
- Im Anhang A, „Technische Spezifikationen“, werden die technischen Daten für die Pipeline aufgeführt.
- Im Anhang B, „Pipeline-Leistungsmerkmale für Sprachrufe“, wird erklärt, wie die Sprachruf-Leistungsmerkmale der Pipeline funktionieren.
- Im Anhang B, „Fehlersuche und -beseitigung“, erfahren Sie, was Sie tun können, wenn es während oder nach der Konfiguration zu Problemen kommt.
- Im Anhang C, „Meldungen über Systemereignisse“, werden die Pipeline-Ereignismeldungen beschrieben.
- Im Anhang D, „ISDN-Fehlercodes“, werden die ISDN-Fehlercodes erläutert.
- Im Anhang E, „Aktualisieren der Systemsoftware“, wird erklärt, wie Sie die Pipeline-Systemsoftware aktualisieren können.
- Im Anhang F, „Ascend-Glossar“, finden Sie Erläuterungen zu Ascend-Netzwerktermini.

Darüber hinaus verfügt dieses Handbuch auch über einen Index.

Voraussetzungen

Dieses Handbuch wendet sich an den Personenkreis, der für die Konfiguration und Wartung der Pipeline verantwortlich ist. Für die Konfiguration der Pipeline sind folgende Kenntnisse erforderlich:

- Internet- bzw. Telearbeitskenntnisse
- WAN (Wide Area Network)-Kenntnisse
- LAN (Local Area Network)-Kenntnisse, falls zutreffend

Hinweise zur typographischen Gestaltung

Dieser Abschnitt enthält Hinweise zur typographischen Gestaltung dieses Handbuchs.

Gestaltungs-element	Bedeutung
`Nichtproportionale Schrift (Courier)`	In nichtproportionaler Schrift (Courier) erscheinen Informationen, die genau so eingegeben werden müssen, wie angegeben. Außerdem wird Text auf dem Bildschirm, wie z. B. statistische Imformationen, auf diese Weise dargestellt.
[]	Eckige Klammern umschließen optionale Attribute, die an einen Befehl angehängt werden. Um ein Attribut anzuhängen, ist nur der Text innerhalb der Klammern einzugeben. Die Klammern selbst sind nur dann mit einzugeben, wenn sie fett gedruckt sind.
Kursiv	Kursivschrift wird zur Darstellung von Variableninformationen verwendet. Statt der kursiv gedruckten Wörter sind die entsprechenden Informationen, für die sie stehen, einzugeben.
Taste1-Taste2	Diese Schreibweise dient zur Darstellung von Tastenkombinationen. Halten Sie die erste Taste gedrückt und drücken Sie dann die nächste(n) Taste(n). Lassen Sie alle Tasten gleichzeitig los.
|	Das Zeichen | trennt Befehle, die sich gegenseitig ausschließen.
Hinweis:	Hinweise enthalten wichtige Zusatzinformationen.
 **Achtung:**	Achtungshinweise enthalten Informationen, deren Nichtbefolgung zu einem Verlust von Daten oder zur Beschädigung von Ausrüstungsteilen führen kann.
 **Warnung:**	Warnhinweise enthalten Informationen zu Sicherheitsvorkehrungen, deren Nichtbefolgung zu Personenschäden führen kann.

Hinweise zur Benutzung dieses Handbuchs

Dieser Abschnitt enthält eine kurze Übersicht darüber, welcher Arbeitsschritt in welchem Kapitel beschrieben wird.

Was möchten Sie tun?	Kapitel
Pipeline installieren	Kapitel 1, „Einführung“
Übersicht über die Pipeline-Leistungsmerkmale und -Fähigkeiten erhalten	Kapitel 2, „Installation der Pipeline“
Grundlegende Konfiguration der Pipeline durchführen und den ISDN-Anschluß einrichten	Kapitel 3, „Pipeline-Grundeinstellungen“
Informationen zur Arbeit mit der VT100-Konfigurationsoberfläche erhalten	Kapitel 4, „Die Pipeline-Benutzeroberfläche“
Seriellen WAN-Anschluß konfigurieren	Kapitel 5, „Konfigurieren von WAN-Verbindungen“
Eine Frame-Relay-Verbindung konfigurieren	Kapitel 5, „Konfigurieren von WAN-Verbindungen“
Informationen zur Beantwortung von eingehenden Rufen durch die Pipeline erhalten	Kapitel 5, „Konfigurieren von WAN-Verbindungen“
PPP- und MPP-Rufe konfigurieren	Kapitel 5, „Konfigurieren von WAN-Verbindungen“
Die Pipeline als eine Brücke konfigurieren und die Bridging-Tabelle verwalten	Kapitel 6, „Konfigurieren der Pipeline als Bridge“
Die Pipeline als einen IP-Router konfigurieren und die Routing-Tabelle verwalten	Kapitel 7, „Konfigurieren der Pipeline als IP-Router“
Die Pipeline als einen IPX-Router konfigurieren	Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“

Was möchten Sie tun?	Kapitel
Die Pipeline-Sicherheitsmaßnahmen einrichten	Kapitel 9, „Einrichten der Pipeline-Sicherheit“
Die Standard-Sicherheitseinstellungen der Pipeline ändern, um sie sicherer zu machen	Kapitel 9, „Einrichten der Pipeline-Sicherheit“
Die Pipeline so einrichten, daß abgehende Sicherheitsrufe unterstützt werden	Kapitel 9, „Einrichten der Pipeline-Sicherheit“
IP-, IPX- oder AppleTalk-Filter einrichten	Kapitel 10, „Definieren von Filtern“
Informationen zur Administration der Pipeline erhalten	Kapitel 11, „Systemadministration“
Mit Hilfe des Terminal-Servers die Routing-Tabellen einsehen und verwalten, Pipeline-Statistiken abrufen und Telnet-Verbindungen zu anderen Geräten am Netz aufbauen	Kapitel 11, „Systemadministration“
Mehr über technische Daten erfahren	Anhang A, „Technische Spezifikationen“
Informationen zu den Sprachruf-Leistungsmerkmalen der Pipeline erhalten	Anhang B, „Pipeline-Leistungsmerkmale für Sprachrufe“
Probleme mit der Pipeline aufspüren und beheben	Anhang B, „Fehlersuche und -beseitigung“
Die ISDN-Fehlercode-Beschreibungen lesen	Anhang D, „ISDN-Fehlercodes“
Informationen zur Aktualisierung der Pipeline-Systemsoftware erhalten	Anhang E, „Aktualisieren der Systemsoftware“
Detaillierte Beschreibungen aller Pipeline-Parameter lesen	*Referenzhandbuch*

Einführung

1

In diesem Kapitel wird die Pipeline vorgestellt und kurz erklärt, was Sie mit ihr tun können. Das Kapitel ist in die folgenden Abschnitte unterteilt:

Funktionen und Leistungsmerkmale

Herzlich willkommen! Mit der Pipeline haben Sie sich für Ascends preisgünstige Heimbüro- und Telearbeitslösung entschieden. Die Pipeline ermöglicht die komplette Nutzung der Netzwerk- und Multimedia-Datenübertragung von Ihrem Heimbüro aus.

Die Pipeline, die nicht größer als ein Modem ist, unterstützt folgendes:

- ISDN-Basisanschluß
- protokollunabhängiges Bridging
- dynamische Bandbreitenzuweisung
- Durchsatzrate von 128 KBit/s durch inverses Multiplexing
- Sicherheitsfunktionen (Einwählsicherheit, PAP, CHAP, Sicherheitskarten)
- Unicast- und Multicast-Paketfilter
- PPP (Point-to-Point Protocol) und MPP (Multichannel Point-to-Point)
- einfache Software-Aktualisierung über Flash-Speicher
- Remote Management von anderen Ascend-Produkten aus, die ebenfalls AMP (Ascend Management Protocol) unterstützen
- Telnet und SNMP
- maximale Durchsatzraten durch Datenkomprimierung (bis zu 512 KBit/s)
- IP-Routing-Software für den Zugang zu Netzwerken auf TCP/IP-Basis, wie das Internet oder Firmennetze, die mit Unix-Computern arbeiten
- IPX-Routing-Software für den Zugang zu Firmennetzen, die über NetWare-Server verfügen

Pipeline-Profile

Zur Speicherung der System- und Verbindungsinformationen verwendet die Pipeline verschiedene Profile.

Systemprofile sind unter dem Menü „System“ zu finden. Diese Profile dienen zur Festlegung von Parametern, die für das Gerät selbst, die Sicherheit und die Administration gelten.

Netzwerkprofile sind im „Ethernet“-Menü zu finden. Mit den Netzwerkprofilen können Sie Parameter für Netzwerkzustände und -verbindungen festlegen. Folgende Netzwerkprofile stehen zur Verfügung:

- Verbindungsprofile („Connections“, für ankommende und abgehende Rufe)
- Bridge-Adreßprofile („Bridge Adrs“, die physikalischen Adressen entfernter Geräte)
- Statische-Routen-Profile („Static Rtes“, statische IP-Routen)
- Filterprofile („Filters“, Paketfilter)
- Frame-Relay-Profile (Verbindung zum Frame-Relay-Switch)
- Antwortprofile („Answer“, ankommende Rufe aus unbekannten Netzen)
- SNMP-Traps-Profile (SNMP-Informationen)
- IPX-Routing-Profile („IPX-Routes“, statische IPX-Routen zu entfernten Servern)
- IPX-SAP-Filter-Profile (NetWare-SAP-Filter)
- Konfigurationsprofile („Mod Config“, lokale Ethernet-Konfiguration)

Verbindungsprofile („Connections“)

Die Verbindungsprofile gelten jeweils für ein bestimmtes Ziel und werden verwendet, um abgehende und ankommende Verbindungen mit diesem Zielnetz herzustellen. Es können Verbindungen zu maximal 8 verschiedenen Orten konfiguriert werden.

Das erste Verbindungsprofil wird automatisch erstellt, sobald Sie die Parameter im Menü „Configure“ festlegen. Im Konfigurationsprofil werden eine Reihe von Parametern festgelegt, die für genau ein entferntes Netzwerk spezifisch sind. Sie können im Menü „Configure“ aber auch einen Hostnamen für die Pipeline und deren ISDN-Merkmale festlegen. Diese Einstellungen gelten für alle Verbindungen.

Bridge-Adreßprofile („Bridge Adrs“)

Wenn der Parameter „Dial Brdcast“ in einem Verbindungsprofil auf „No“ gesetzt wurde, initiiert die Pipeline keine Verbindungen für Broadcast-Anforderungen (z. B., wenn eine lokale Anwendung eine Broadcast-Meldung zur Suche nach einem Server sendet). Statt dessen werden die in den Bridge-Adreßprofilen („Bridge Adrs“) angegebenen Ziele verwendet.

Statische-Routen-Profile („Static Rtes“)

Wenn die Pipeline so konfiguriert wurde, daß Sie IP-Protokolle routen soll, kann sie mit Hilfe von RIP (Routing Information Protocol) Routing-Informationen über das lokale und das entfernte Netzwerk empfangen und senden. Wurde RIP in einem Verbindungsprofil deaktiviert, verwendet die Einheit statt dessen die im Statische-Routen-Profil („Static Rtes“) konfigurierten statischen Routen. Die Verbindungsprofile erscheinen in der Routing-Tabelle der Pipeline jeweils als eine statische Route.

Filterprofile

Das Haupteinsatzgebiet von Filterprofilen ist die Aussonderung von Datenpaketen, die nicht über die ISDN-Verbindung übertragen werden müssen, so daß unnötige Verbindungen nicht erst aktiviert werden. Da die Pipeline Verbindungen automatisch (und „stillschweigend“) je nach der Netzwerkaktivität initiiert, kann der routinemäßige Netzwerkverkehr, wie z. B. der Broadcast-Verkehr, Verbindungen unnötigerweise aufbauen oder aufrechterhalten. Mit Hilfe eines Filters kann der routinemäßige Broadcast- bzw. Multicast-Verkehr im Netz herausgefiltert werden, um zu verhindern, daß diese Pakete die Verbindung aufrechterhalten. Solcherart verwendete Filter werden Ruffilter genannt.

Die Pipeline enthält vordefinierte Ruffilter für NetWare-, TCP/IP- und AppleTalk-Verbindungen. Filter können darüber hinaus auch dazu benutzt werden, bestimmte Arten von Daten an der lokalen bzw. der ISDN-Schnittstelle auszusondern oder ankommende Pakete abzuweisen, die an bestimmte Hosts adressiert sind. Das Aussondern von Verkehr auf diese Art und Weise erfolgt mit sogenannten Datenfiltern.

Frame-Relay-Profile

Für stark beanspruchte Netzwerke unterstützt die Pipeline sowohl Frame Relay als auch gewählte Verbindungen. Zur Konfiguration von Frame-Relay-Verbindungen stehen Ihnen die Frame-Relay-Profile zur Verfügung.

Antwortprofile („Answer“)

Wenn die Pipeline einen ankommenden Datenruf empfängt, überprüft sie zunächst, ob der ankommende Ruf die erforderliche Authentifizierung (falls es eine solche gibt) unterstützt. Die erforderliche Authentifizierung wird im Antwortprofil festgelegt.

Die Pipeline sucht dann nach einem Verbindungsprofil, das der Kennung des ankommenden Rufes entspricht. Findet sie ein entsprechendes Verbindungsprofil, verwendet sie die Konfigurationseinstellungen im Verbindungsprofil für den Ruf.

Kann die Pipeline kein Verbindungsprofil für den Ruf finden, versucht sie, die Konfigurationseinstellungen im Antwortprofil zu verwenden.

SNMP-Traps-Profile

In SNMP-Traps-Profilen können Sie die IP-Adresse von SNMP-Management-Computern sowie andere Parameter festlegen. So kann z. B. festgelegt werden, ob Alarme gesendet werden sollen.

IPX-Routing-Profile

IPX-Routing-Profile enthalten alle für das Erreichen eines bestimmten IPX-Dienstes im entfernten Netz erforderlichen Informationen. IPX-Routing-Profile werden z. B. für IPX-Netze benötigt, bei denen es lange dauern kann, bis Clients einen Server finden (zur Vermeidung von Zeitlimitüberschreitungen). Es wird empfohlen, beim Einsatz von IPX-Routing mindestens ein IPX-Routing-Profil zu konfigurieren.

IPX-SAP-Filterprofile

In NetWare 4.0 und höher ist SAP aufgrund der integrierten Verzeichnisdienste nicht mehr erforderlich, da die Dienste über Verzeichnisdienste angesteuert werden.

In NetWare 3.*x* senden die NetWare-Server jedoch alle 60 Sekunden SAP-Pakete, um sicherzustellen, daß allen Routern und Bridges die verfügbaren Dienste bekannt sind.

Wie andere IPX-Router auch, erstellt die Pipeline auf der Grundlage der statisch konfigurierten IPX-Routen und der in den SAP-Broadcast-Paketen enthaltenen Informationen eine Dienstetabelle. In einer aktiven IPX-Umgebung beinhaltet dies viele Server und viele Serverarten, so daß die Dienstetabelle sehr groß sein kann. IPX-SAP-Filter versetzen die Pipeline in die Lage, die Dienstetabelle auf eine verwaltbare Größe zu beschränken, und bieten darüber hinaus ein größeres Maß an Kontrolle für den Netzwerkadministrator.

Ethernet-Profil („Mod Config“)

Das lokale Ethernet-Netzwerk verfügt über bestimmte Standardwerte, die im Konfigurationsprofil festgelegt sind. Diese können jedoch mit Hilfe von IP- oder IPX-Routing-Parametern, Informationen über die Meldungsprotokollierung und anderen lokalen Optionen konfiguriert werden. Wenn Sie Verbindungen zu entfernten IP- bzw. IPX-Netzwerken herstellen, müssen Sie die lokalen IP- bzw. IPX-Parameter in diesem Profil angeben.

Sicherheitsfunktionen

Die Pipeline-Software verfügt über verschiedene Sicherheitsfunktionen. Dieser Abschnitt gibt einen kurzen Überblick über diese Funktionen. Ausführlichere Informationen finden Sie im

- PAP und CHAP

  Die Pipeline unterstützt die beiden Sicherheitsprotokolle PAP (Password Authentication Protocol) und CHAP (Challenge Handshake Authentication Protocol).

- Beschränkungen für ankommende Rufe

  Sie können die Pipeline so konfigurieren, daß ankommende Rufe von unbekannten Netzen nicht beantwortet werden. Die Beschränkung des Netzzugriffs auf die Pipeline bietet eine hohe Sicherheit gegen den unbefugten Netzzugriff von außerhalb.

- Rückruf

  Wenn in einem Verbindungsprofil die Rückruf-Funktion (Parameter „Callback“) aktiviert wurde, hängt die Pipeline sofort nach dem Empfang eines ankommenden Rufs auf und initiiert einen Ruf zum entfernten Ende. Die Rückruf-Funktion bietet die höchste Sicherheit, da sichergestellt ist, daß alle ankommenden Rufe aus einem bekannten Netz heraus erfolgen.

- Authentifizierung per Sicherheitskarte

  Die Pipeline unterstützt die Verwendung von persönlichen Sicherheitskarten, wie z. B. die der Firmen Enigma Logic® und Security Dynamics®. Diese Karten verfügen über dynamische Kennwörter, die ein höheres Maß an Sicherheit bieten als bei den herkömmlichen Verfahren mit festen Kennwörtern. Die Unterstützung dynamischer Kennwörter erfordert die Verwendung eines RADIUS-Servers, der (in der Zentrale) Zugang zu einem Authentifizierungsserver hat. Beispiele für Authentifizierungsserver sind der Enigma Logic SafeWord AS und der Security Dynamics ACE-Server.

- Mehrstufige Zugriffssicherheit über Benutzerkennwörter

  Die Zugriffssicherheit für die Pipeline wird über Sicherheitsprofile festgelegt. In jedem Sicherheitsprofil können Sie den Zugriff auf wichtige Pipeline-Operationen einschränken, während andere, weniger wichtige Anwendungen weiterhin verfügbar bleiben.

- Filterung von Paketen

  Die Pipeline verfügt über einen Filtermechanismus, mit dessen Hilfe Sie Ihre Einwähl-Netzwerkumgebung sichern können. Filter können sowohl für Schnittstellen als auch für einzelne Verbindungen festgelegt werden. Filter dienen zur Feststellung,

  – ob der Ruf aufgebaut werden soll,
  – ob der Ruf getrennt werden soll,
  – ob Daten übertragen werden sollen oder
  – ob Daten angenommen werden sollen.

  Jeder Filter besteht aus einer geordneten Liste der Parameter auf der Grundlage von IP-, IPX- oder protokollunabhängigen Informationen.

Weitere Informationen zu Filtern finden Sie in Kapitel 10, „Definieren von Filtern“.

Verwaltung Ihrer Pipeline

Die primäre Konfigurationsschnittstelle für die Pipeline ist ein zeichenorientierter VT-100-Bildschirm, mit dessen Hilfe Sie die Einstellungen für Ihre Pipeline konfigurieren und den Status der Einheit überwachen können. Der Zugriff auf diese Schnittstelle erfolgt über den seriellen Anschluß Ihres Computers mit Hilfe eines VT-100 unterstützenden Terminalemulationsprogramms.

Die Pipeline-Software verfügt über die folgenden Verwaltungsmechanismen:

- Telnet-Management

  Sie können eine Pipeline von einem entfernten Standort aus verwalten, indem Sie von jeder beliebigen Telnet-Workstation im Unternehmensnetz aus eine Telnet-Sitzung herstellen. Nach Eingabe des entsprechenden Kennwortes können Sie mittels eines VT-100-Fenster auf die Benutzerschnittstelle der Pipeline zugreifen und sämtliche von einem lokalen Terminal aus möglichen Konfigurations-, Diagnose-, Verwaltungs- und andere Steuerfunktionen ausführen.

- SNMP-Management

  Die Pipeline unterstützt SNMP-Traps, so daß sie auf diese Weise Alarme, Berichte zu Gesprächsdetails und andere Verwaltungsinformationen an einen SNMP-Manager senden kann, ohne daß diese abgefragt werden müssen.

- Software-Aktualisierungen per FLASH-Speicher

  Der FLASH EEPROM der Pipeline macht eine Aktualisierung der Software am Standort der Einheit möglich, ohne daß dazu die Einheit geöffnet oder Speicherchips geändert werden müssen. Die Aktualisierung der Pipeline-Software erfolgt über den seriellen Terminal-Anschluß.

- DO-Menü

  Wenn Sie in einem Konfigurationsmenü die Tastenkombination Strg-D drücken, öffnet sich das DO-Menü. Mit Hilfe des DO-Menüs können Sie z. B. Rufe manuell wählen bzw. beenden oder Sicherheitsstufen für die Pipeline ändern.

- Befehle zur Systemdiagnose

  Die Pipeline-Software verfügt über Befehle zum Neustarten des Geräts, Speichern und Wiederherstellen der Konfigurationsinformationen und Ausführen anderer administrativer Aufgaben.

- Terminal-Server-Schnittstelle

  Sie können eine Befehlszeilenoberfläche aufrufen, von der aus Verbindungen getestet, Routing-Tabellen und andere Parameter überprüft oder die Konfiguration der Pipeline von einem entfernten Standort aus aktiviert werden können.

- Statusfenster

  Anhand der Statusfenster der Systemsoftware ist ersichtlich, was gegenwärtig in der Pipeline abläuft. In einem der Statusfenster werden z. B. bis zu 31 der letzten Systemereignisse angezeigt, die seit dem Einschalten der Pipeline aufgetreten sind, während in einem anderen statistische Angaben über die gegenwärtig aktive Sitzung zu sehen sind. Darüber hinaus gibt es auch einige aktive Funktionen, die Sie im Statusfenster ausführen können, wie z. B. das manuelle Beenden einer aktiven Verbindung.

Aufbau von Pipeline-Verbindungen

In diesem Abschnitt werden kurz einige der Elemente erläutert, die sich darauf auswirken, wie die Pipeline Verbindungen aufbaut.

Initiieren von Sitzungen

Eine Sitzung ist eine aktive Verbindung. Die Pipeline initiiert Sitzungen mit einem entfernten Netz im Normalfall „auf Anforderung“, also auf der Grundlage des aktiven Verkehrs (an ein entferntes Netz gesendete oder von dort empfangene Pakete). Der routinemäßige Verkehr kann u. U. Verbindungen von selbst aufbauen, die zu unnötigen Verbindungskosten führen. Um dies zu verhindern, können Sie Filter einsetzen. Sitzungen können aber auch mit Hilfe des DO-Menüs manuell gestartet werden.

Die Pipeline baut eine Sitzung mit einem entfernten Gerät auf, indem sie das Gerät anwählt (bzw. einen ankommenden Ruf annimmt) und dann mit diesem Gerät Informationen austauscht, um sicherzustellen, daß die Kommunikation auch wirklich zustandekommt. Beide Seiten der Verbindung müssen gleich konfiguriert sein, um die Sitzung aufbauen zu können.

Während der oben beschriebenen Handshake-Prozedur werden die folgenden Informationen ausgetauscht:

- Optionen der Telefongesellschaft
- Einkapselungsoptionen (gemeinsame Festlegung, wie der Datenaustausch erfolgen soll)
- Authentifizierungsoptionen
- Datenkomprimierungsoptionen
- Bridging- oder/und Routing-Informationen

Telefongesellschaftsspezifische Optionen

Die meisten der telefongesellschaftsspezifischen Optionen („Telco options“), die mit ISDN zu tun haben, beziehen sich auf die Art des von Ihrem ISDN-Anschluß unterstützten Datendienstes und sind auf Standardwerte eingestellt, die Rufe innerhalb Nordamerikas möglich machen.

Die Pipeline geht standardmäßig von einem 56K-Datendienst auf jedem der ISDN-Kanäle aus, da auf dem Weg zu europäischen Ländern bzw. zu den Pazifikanrainerstaaten nicht vollständig ein 64K-Datendienst gewährleistet werden kann. Wenn Ihre Verbindung von Ende zu Ende 64K unterstützt, können Sie die Pipeline für den 64K-Datendienst konfigurieren.

(Hinweis: In Deutschland, Österreich und der Schweiz: 64K)

Einkapselungsoptionen

Für die Verbindung zwischen der Pipeline und entfernten Standorten kommt das Protokoll PPP (Point-to-Point Protocol) zum Einsatz. Eine Verbindung kann nur zustandekommen, wenn die andere Seite ebenfalls PPP unterstützt.

Die Pipeline unterstützt sowohl das Standard-PPP als auch eine Mehrkanalversion dieses Protokolls mit dem Namen MPP (Multichannel Point-to-point Protocol), die das Invers-Multiplexing, die dynamische Bandbreitenzuweisung und die Kanalüberwachung und -ersetzung unterstützt. Die Arbeitsweise der Funktionen können Sie mit Hilfe von Konfigurationseinstellungen Ihren Wünschen entsprechend anpassen.

Wenn Sie die Pipeline für MPP (Standard) konfigurieren, MPP aber vom entfernten Netzwerk nicht unterstützt wird, handelt das Gerät eine Multilink-PPP-Verbindung aus, und falls dies nicht gelingt, wird zum Standard-PPP zurückgekehrt.

Authentifizierungsoptionen

Die Authentifizierung ist ein wichtiger Teil beim Aushandeln einer Sitzung zwischen den beiden Seiten. Häufig muß ein Kennwort angegeben werden, damit eine Sitzung zustandekommt. Eine ausführliche Beschreibung der von der Pipeline unterstützten Sicherheitsmaßnahmen finden Sie im Abschnitt „Sicherheitsfunktionen“ auf Seite 1-6.

Optionen für die Datenkomprimierung

Die Pipeline unterstützt die Komprimierungsverfahren STAC, Microsoft LZS Coherency Compression für Windows 95 und Van-Jacobsen-Komprimierung.

Bei der STAC-Komprimierung wird ein von der Firma STAC Electronics, Inc. entwickelter Komprimierungsalgorithmus verwendet, der den Standard-LZS-Komprimierungsalgorithmus so modifiziert, daß die Komprimierungsgeschwindigkeit erhöht wird (zu Lasten des Komprimierungsgrads). Wenn Sie für das Gerät STAC-Komprimierung festlegen und das Gerät am anderen Ende ebenfalls STAC-Komprimierung unterstützt, wird diese beim Aushandeln einer PPP-Verbindung eingerichtet.

Microsoft LZS Coherency Compression für Windows 95 ist ein nur unter Windows 95 (nicht unter Windows NT) einsetzbares proprietäres Komprimierungsverfahren.

Beim Van-Jacobsen-Verfahren kommt ein Header-Komprimierungsalgorithmus zum Einsatz, der ursprünglich für TCP/IP entwickelt wurde, inzwischen aber sowohl für TCP/IP als auch für IPX einsetzbar ist, und die Größe der Paketheader reduziert, wodurch die Leitungen effizienter genutzt werden können.

Bridging und Routing

Die Pipeline kann sowohl als Bridge als auch als Router eingesetzt werden. Mit Hilfe des protokollunabhängigen Bridging können auch andere Protokolle als IP und IPX, wie z. B. AppleTalk, verwendet werden. Routing und Bridging sind über jede Verbindung gleichzeitig einsetzbar.

Wenn Sie eine Routing-Konfiguration zu einem zweiten Ziel (einem anderen Ziel als dem im Konfigurationsprofil angegebenen) festlegen, ist darauf zu achten, daß *beide Seiten* der Verbindung mit Routing-Informationen konfiguriert sein müssen. Informationen zum entfernten Netzwerk werden im Verbindungsprofil für das Zielnetz gespeichert, während die Netzwerkinformationen für das lokale Ethernet-Netzwerk im Ethernet-Profil konfiguriert werden.

Wie geht's weiter?

In Kapitel 2, „Installation der Pipeline", finden Sie Informationen dazu, wie Sie Ihre Pipeline installieren können.

Installation der Pipeline

2

Dieses Kapitel enthält die folgenden Abschnitte:

Inhalt des Pipeline-Pakets

Das Pipeline-Paket enthält die folgenden Komponenten:

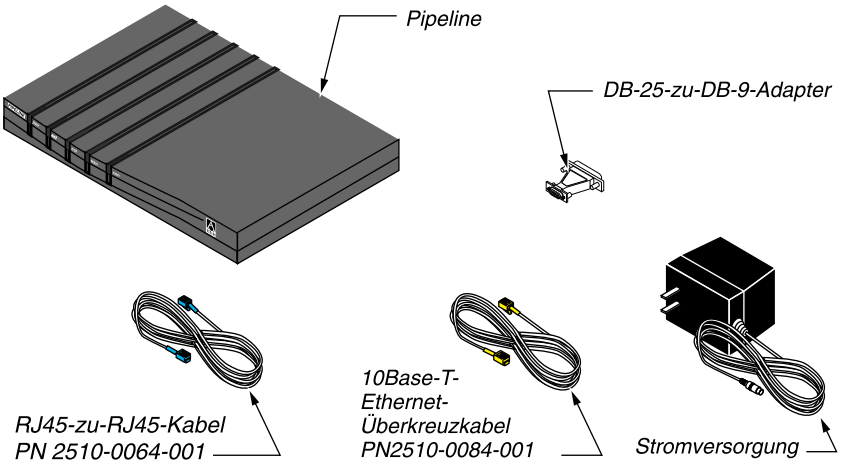


Abbildung 2-1: Hardware im Pipeline-Paket

- Die Pipeline.
- Ein RJ-45-zu-RJ-45-ISDN-Kabel (Teile-Nr. 2510-0064-001).

  An den Enden dieses Kabels befinden sich zwei unterschiedlich große Stekker. Der größere der beiden Stecker ist ein RJ-45-Stecker für den WAN-Anschluß der Pipeline; der kleinere Stecker ist ein RJ-45-Stecker für Ihre ISDN-Telefondose.
- Ein 10Base-T-Ethernet-Überkreuzkabel (Teile-Nr. 2510-0084-001).

  Wird die Pipeline nur mit einem Computer zusammen eingesetzt, und verfügt dieser Computer über eine 10Base-T-Ethernet-Schnittstelle, können Sie den Computer mit diesem Kabel direkt mit der 10Base-T-Ethernet-Buchse der Pipeline verbinden (Näheres dazu weiter unten). *Dieses Kabel kann nur für diesen Zweck eingesetzt werden.*

- Ein serielles DB-9–zu–DB-25-Adapterkabel (Teile-Nr. 2510-0052-002). Dieses Kabel dient zur Verbindung des Terminal-Anschlusses der Pipeline mit einem der seriellen Anschlüsse des Computers (Näheres dazu weiter unten).
- Ein Netzteil.
- Zwei Handbücher: dieses (*Pipeline 50 – Benutzerhandbuch*) und das *Referenzhandbuch*.
- Eine Registrierungskarte.

Außer den Teilen, die sich in Ihrem Pipeline-Paket befinden, benötigen Sie zusätzliche Hardware-Komponenten und Software, die in den nächsten beiden Abschnitten beschrieben werden.

Zusätzlich benötigte Hardware

Außer den Hardware-Komponenten, die zusammen mit der Pipeline geliefert werden, benötigen Sie zur Installation Ihrer Pipeline weiterhin die in diesem Abschnitt beschriebene Hardware.

WAN-Schnittstelle

Je nachdem, was für ein Pipeline-Modell Sie haben, benötigen Sie eine ISDN-Wählleitung oder eine Standleitung. Informationen zur Bestellung eines ISDN-Anschlusses können Sie dem Dokument „Ordering ISDN Service“ entnehmen, das Sie zusammen mit der Pipeline erhalten haben.

Externer Netzabschluß (NTBA, nur bei Geräten mit S-Schnittstelle)

(In Deutschland, Österreich und der Schweiz ist dies der Fall.) Wenn Ihre Pipeline eine S-Schnittstelle hat, benötigen Sie einen externen ISDN-Netzabschluß (Network Terminator, NT1). Einen externen Netzabschluß benötigen Sie auch dann, wenn an einen ISDN-Anschluß mehr als ein ISDN-Gerät angeschlossen wird.

Was für eine ISDN-Schnittstelle Ihre Pipeline hat, können Sie anhand der Modellnummer auf der Verpackung bzw. an der Unterseite des Geräts feststellen:

- Lautet die Modellnummer P50-1UBRI, hat Ihre Pipeline eine U-Schnittstelle.
- Lautet die Modellnummer P50-1SBRI, hat Ihre Pipeline eine S-Schnittstelle.

Computer mit seriellem Anschluß

Zur Konfiguration und Überwachung der Pipeline benötigen Sie einen Computer mit einem seriellen COM-Anschluß, der Daten mit einer Geschwindigkeit von 9600 Bits pro Sekunde übertragen kann. Der serielle COM-Anschluß wird im Normalfall z. B. zum Anschluß eines externen Modems verwendet. Sollten Sie weitere Informationen zu den seriellen Anschlüssen Ihres Computers benötigen, finden Sie diese im Handbuch zu Ihrem Computer.

Wenn möglich sollte einer der seriellen Anschlüsse ständig für die Pipeline reserviert sein, um eine Dauerverbindung zwischen Pipeline und Computer herzustellen. Eine solche Dauerverbindung ist zwar für die Kommunikation mit dem entfernten Netz nicht unbedingt erforderlich, aber sie ermöglicht es Ihnen jederzeit, die Arbeit der Pipeline zu überwachen, manuell Verbindungen mit entfernten Netzen herzustellen oder solche Verbindungen wieder zu trennen und gegebenenfalls Änderungen der Konfiguration vorzunehmen.

Modemkabel

Für die Verbindung zwischen der Pipeline und dem seriellen Anschluß Ihres Computers benötigen Sie ein Modemkabel (serielles Datenübertragungskabel für den Anschluß eines externen Modems). Das Kabel muß ein Hochgeschwindig-

keitsmodemkabel sein, also eines, das den Hardware-Handshake unterstützt. Dieses Verfahren wird von beinahe allen heute hergestellten Modems verwendet. Dieses Kabel muß auf der einen Seite über einen entsprechenden Stecker für den seriellen COM-Anschluß Ihres Computers verfügen. Der Stecker auf der anderen Seite muß ein 9- bzw. 25poliger D-Stecker sein.

Ethernet-Schnittstelle

Damit die Pipeline Daten an den Computer senden und von diesem empfangen kann, muß Ihr Computer über eine ordnungsgemäß konfigurierte 10Base-T-(Twisted-Pair)- bzw. Thinnet-Ethernet-Schnittstelle verfügen. Dabei kann es sich entweder um eine interne Schnittstelle im Computer oder um eine Adapter- oder PCMCIA-Karte (PC Card) in Ihrem Laptop handeln. Zur Installation der Schnittstelle sind die Anweisungen in der Dokumentation zur Schnittstelle bzw. zum Computer zu befolgen.

Zusätzlich benötigte Software

In diesem Abschnitt wird die Software beschrieben, die Sie für die Arbeit mit der Pipeline zusätzlich benötigen.

Netzwerk-Software

Für den Anschluß an ein Netzwerk muß auf Ihrem Computer die entsprechende Netzwerk-Software installiert sein. Welche Software das ist, hängt von der Art des Netzwerkes ab, mit dem Sie eine Verbindung herstellen wollen:

- Für den Anschluß an ein Novell-IPX-Netzwerk benötigen Sie IPX-Client-Software.
- Für den Anschluß an das Internet oder ein TCP/IP-Netzwerk, benötigen Sie Software, die das Protokoll TCP/IP unterstützt. Solche Netzwerksoftware ist Bestandteil vieler Betriebssysteme, wie z. B. Windows 95 und neuerer Macintosh-Betriebssystemsoftware. Enthält Ihr Betriebssystem keine TCP/IP-Software, muß ein entsprechendes Software-Paket installiert werden.
- Die für den Anschluß an ein AppleTalk-Netzwerk benötigte AppleTalk- und TCP/IP-Software ist bereits Bestandteil des Betriebssystems neuerer Macintoshs.

Wenn die entsprechende Netzwerk-Software installiert ist, müssen Sie so konfigurieren, daß sie mit der Pipeline und dem entfernten Netzwerk kommunizieren kann. Siehe „Konfiguration des Computers“ auf Seite 3-9.

Sollten Sie Fragen dazu haben, welche Software auf Ihrem Computer installiert ist, wenden Sie sich bitte an Ihren Netzwerkadministrator bzw. Ihren Internet-Service-Provider (ISP).

DFÜ-Software

Zur Konfiguration und Überwachung der Pipeline muß auf Ihrem Computer ein DFÜ-Programm (DFÜ = Datenfernübertragung) installiert sein. Mit diesem Programm können Sie auf die Konfigurationsschnittstelle der Pipeline zugreifen. Dazu muß es die folgenden Funktionen und Leistungsmerkmale aufweisen:

- VT100-Terminal-Emulation
- Möglichkeit, die Pipeline statt über ein Modem direkt mit dem Computer zu verbinden (über einen seriellen Anschluß, an den die Pipeline angeschlossen wird; siehe „Anschließen eines Computers an den Terminal-Anschluß der Pipeline“ auf Seite 2-17).

Die meisten DFÜ-Programme, die einzeln erhältlich sind, wie z. B. das Programm PROCOMM PLUS für Microsoft Windows, arbeiten zuverlässig. Für Macintosh-Computer ist das Shareware-DFÜ-Programm ZTerm zu empfehlen.

Achtung: Die Programme „Terminal“ in Microsoft Windows 3.1 und „HyperTerminal“ in Microsoft Windows 95 sind für die Konfiguration der Pipeline nicht zuverlässig genug.

Überblick über die Installation

Im folgenden wird erklärt, wie Sie bei der Installation der Pipeline vorzugehen haben. Die Installationsprozedur läßt sich in die folgenden großen Schritte unterteilen, die in jedem Fall in der angegebenen Reihenfolge auszuführen sind:

1 „Auswählen des Standorts der Pipeline“: Erklärung auf Seite 2-8

2 „Anschließen der Pipeline an den ISDN-Anschluß“: Erklärung auf Seite 2-8

3 „Anschließen der Pipeline an die Ethernet-Schnittstelle des Computers“: Erklärung auf Seite 2-11

oder

„Anschließen an ein Ethernet-Netzwerk“: Erklärung auf Seite 2-12

4 „Anschließen eines Computers an den Terminal-Anschluß der Pipeline“: Erklärung auf Seite 2-17

5 „Starten der Pipeline“: Erklärung auf Seite 2-22

Nach der erfolgreichen Installation der Pipeline können Sie mit der Konfiguration fortfahren. Diese wird im Kapitel 3, „Pipeline-Grundeinstellungen“, erläutert.

Abbildung 2-2 zeigt die Rückseite der Pipeline.

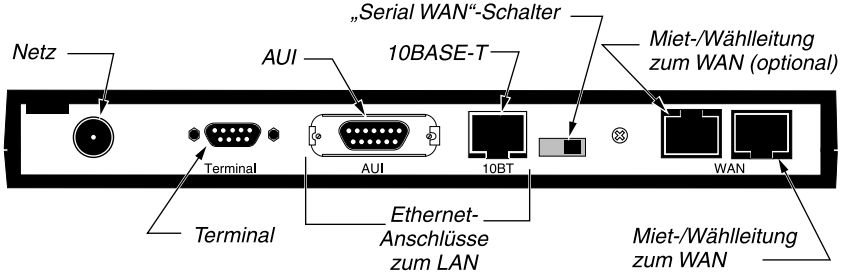


Abbildung 2-2: Rückseite der Pipeline

In den folgenden Abschnitten wird erklärt, wie Sie die entsprechenden Kabel mit diesen Anschlüssen verbinden.

Auswählen des Standorts der Pipeline

Wenn möglich, sollte die Pipeline so aufgestellt werden, daß Sie die Leuchtanzeigen an der Vorderseite des Geräts sehen können. Anhand dieser Leuchtanzeigen läßt sich der aktuelle Status der Pipeline ersehen, z. B. ob der ISDN-Anschluß gerade benutzt wird. Diese Informationen können Ihnen bei der Diagnose von Problemen behilflich sein.

Anschließen der Pipeline an den ISDN-Anschluß

Der erste Schritt bei der Installation der Pipeline besteht im Anschließen der Einheit an Ihren ISDN-Anschluß. Wie dabei vorzugehen ist, hängt davon ab, was für eine Pipeline-Version Sie haben. Die jeweilige Version läßt sich anhand der Modellnummer feststellen.

Die Modellnummer finden Sie entweder auf der Pipeline-Verpackung oder aber an der Unterseite der Einheit.

- Hat Ihre Pipeline die Modellnummer P50-1UBRI, verfügt sie über eine U-Schnittstelle. In diesem Fall gelten für den Anschluß der Pipeline an den ISDN-Anschluß die Anweisungen im folgenden Abschnitt „Anschließen einer Pipeline mit U-Schnittstelle“ auf Seite 2-8.
- Hat Ihre Pipeline die Modellnummer P50-1SBRI, verfügt sie über eine S-Schnittstelle. In diesem Fall gelten für den Anschluß der Pipeline an den ISDN-Anschluß die Anweisungen im Abschnitt „Anschließen einer Pipeline mit S-Schnittstelle“ auf Seite 2-10.

Anschließen einer Pipeline mit U-Schnittstelle

Zum Anschließen einer Pipeline mit einer U-Schnittstelle an den ISDN-Anschluß ist wie folgt vorzugehen:

1 Stecken Sie das Ende des RJ-48C-zu-RJ-11-ISDN-Kabels (Teile-Nr. 2510-0122-001) mit dem größeren Stecker in den WAN-Anschluß an der Rückseite der Pipeline.

Die Enden dieses Kabels sind blau.

2 Stecken Sie das andere Ende des Kabels in die ISDN-Wandsteckdose.

Warnung: Zur Verbindung zwischen Pipeline und ISDN-Anschluß darf *auf keinen Fall* ein 10Base-T-Ethernet-Kabel, wie z. B. das mitgelieferte Überkreuzkabel (Teile-Nr. 2510-0084-001), verwendet werden. Die Verwendung eines falschen Kabels kann zur Beschädigung oder Zerstörung der Pipeline führen.

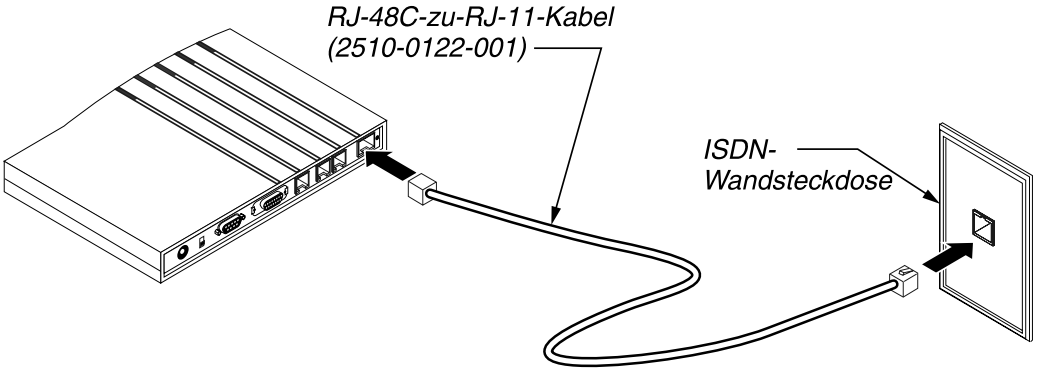


Abbildung 2-3: Verbinden einer Pipeline mit U-Schnittstelle mit dem ISDN-Anschluß

Wie geht's weiter?

- Soll die Pipeline nur mit einem Computer zusammen verwendet werden, können Sie mit dem Abschnitt „Anschließen der Pipeline an die Ethernet-Schnittstelle des Computers“ auf Seite 2-11 fortfahren.
- Soll die Pipeline innerhalb eines Computer-Netzwerks verwendet werden, sind die Anweisungen im Abschnitt „Anschließen an ein Ethernet-Netzwerk“ auf Seite 2-12 zu befolgen.

Anschließen einer Pipeline mit S-Schnittstelle

Zum Anschließen einer Pipeline mit einer S-Schnittstelle an den ISDN-Anschluß ist wie folgt vorzugehen:

1 Stecken Sie das Ende des RJ-45-zu-RJ-45-ISDN-Kabels (Teile-Nr. 2510-0064-001) mit dem größeren Stecker in den WAN-Anschluß an der Rückseite der Pipeline.

Warnung: Zur Verbindung zwischen Pipeline und ISDN-Anschluß darf *auf keinen Fall* ein 10Base-T-Ethernet-Kabel, wie z. B. das mitgelieferte Überkreuzkabel (Teile-Nr. 2510-0084-001), verwendet werden. Die Verwendung eines falschen Kabels kann zur Beschädigung oder Zerstörung der Pipeline führen.

2 Stecken Sie das andere Ende des Kabels in die entsprechende Buchse des externen Netzabschlußgeräts (NT-1) für Ihre ISDN-Verbindung. Siehe dazu die Dokumentation zu Ihrem NT-1.

3 Verbinden Sie den externen NT-1 mit der ISDN-Wandsteckdose. Siehe dazu die Dokumentation zu Ihrem NT-1.

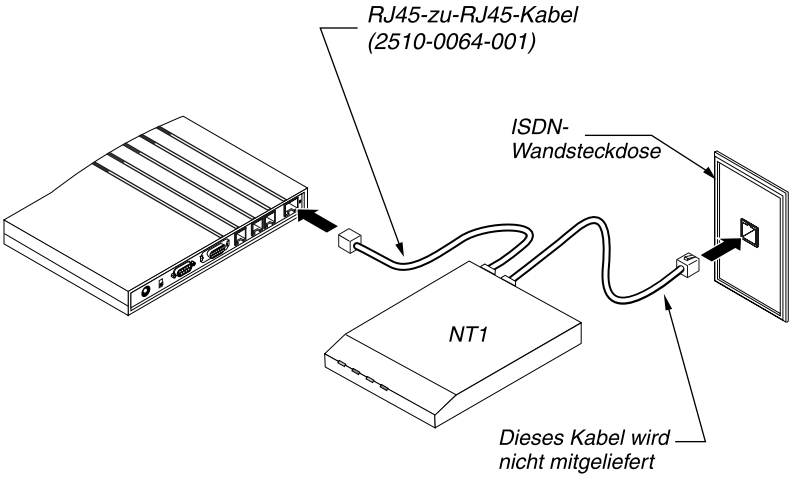


Abbildung 2-4: Anschließen einer Pipeline mit S-Schnittstelle an den ISDN-Anschluß

Wie geht's weiter?

- Soll die Pipeline nur mit einem Computer zusammen verwendet werden, können Sie mit dem Abschnitt „Anschließen der Pipeline an die Ethernet-Schnittstelle des Computers“ auf Seite 2-11 fortfahren.
- Soll die Pipeline innerhalb eines Computer-Netzwerks verwendet werden, sind die Anweisungen im Abschnitt „Anschließen an ein Ethernet-Netzwerk“ auf Seite 2-12 zu befolgen.

Anschließen der Pipeline an die Ethernet-Schnittstelle des Computers

Wird die Pipeline nur mit einem Computer zusammen eingesetzt, und verfügt dieser Computer über eine 10Base-T-(Twisted-Pair-)Ethernet-Schnittstelle, können Sie Pipeline und Computer mit Hilfe des mitgelieferten speziellen 10Base-T-Kabels, auch *Überkreuzkabel* genannt, miteinander verbinden.

1 Stecken Sie das eine Ende des 10Base-T-Überkreuzkabels (Teile-Nr. 2510-0084-001) in die 10BT-Buchse an der Rückseite der Pipeline.

2 Stecken Sie das andere Ende des Kabels in die 10Base-T-Ethernet-Buchse des Computers.

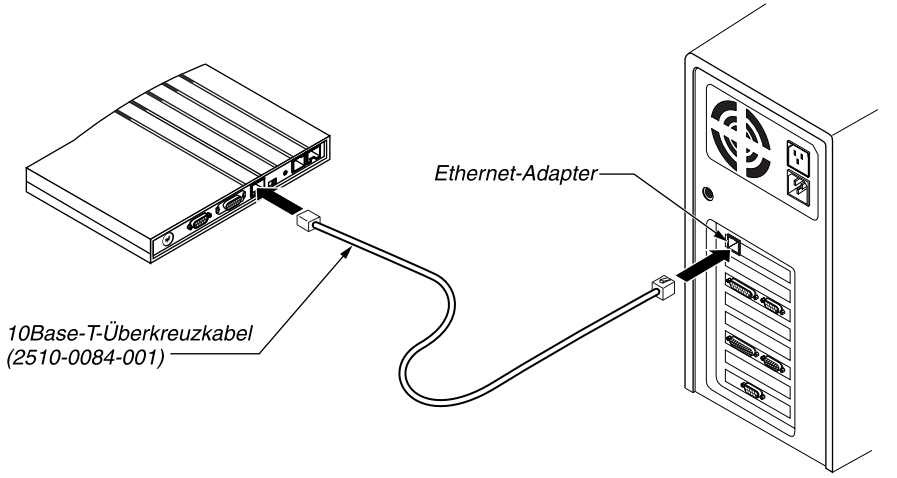


Abbildung 2-5: Anschließen der Pipeline an die Ethernet-Schnittstelle des Computers

Wie geht's weiter?

- Fahren Sie mit den Anweisungen im Abschnitt „Anschließen eines Computers an den Terminal-Anschluß der Pipeline“ auf Seite 2-17 fort.

Anschließen an ein Ethernet-Netzwerk

- Zum Anschließen der Pipeline an ein 10Base-T-(Twisted-Pair-)Ethernet-Netzwerk mit einem Hub siehe „Anschließen an ein 10Base-T-Netzwerk mit einem Hub“ auf Seite 2-12.
- Zum Anschließen der Pipeline an ein Thinnet-(10Base-2-)Ethernet-Netzwerk siehe „Anschließen an ein Thinnet-Netzwerk“ auf Seite 2-14.

Anschließen an ein 10Base-T-Netzwerk mit einem Hub

Zum Anschließen der Pipeline an ein 10Base-T-Netzwerk mit einem Hub gehen Sie wie folgt vor:

1 Stecken Sie das eine Ende eines 10Base-T-Kabels in die 10BT-Buchse der Pipeline.

Achtung: Zum Anschließen der Pipeline an ein 10Base-T-Netzwerk mit einem Hub darf nicht das mitgelieferte 10Base-T-Überkreuzkabel (Teile-Nr. 2510-0084-001) verwendet werden. Dieses Kabel dient ausschließlich zum direkten Verbinden der Pipeline mit einem Computer (siehe „Anschließen der Pipeline an die Ethernet-Schnittstelle des Computers“ auf Seite 2-11).

2 Stecken Sie das andere Ende des Kabels in einen freien Anschluß am 10Base-T-Hub.

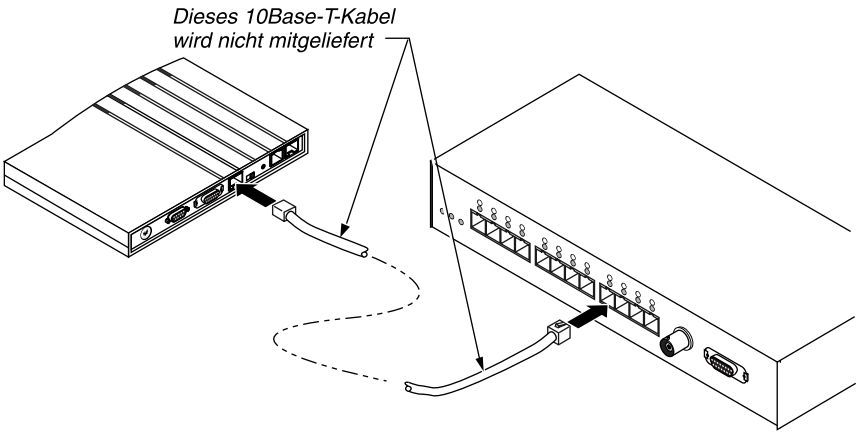


Abbildung 2-6: Verbinden des 10Base-T-Kabels mit dem Hub

Wie geht's weiter?

- Fahren Sie mit den Anweisungen im Abschnitt „Anschließen eines Computers an den Terminal-Anschluß der Pipeline“ auf Seite 2-17 fort.

Anschließen an ein Thinnet-Netzwerk

Zum Anschließen der Pipeline an ein Thinnet-(10Base-2-)Netzwerk ist wie folgt vorzugehen:

1 Schließen Sie einen Thicknet-zu-Thinnet-Transceiver an die AUI-Buchse der Pipeline an.

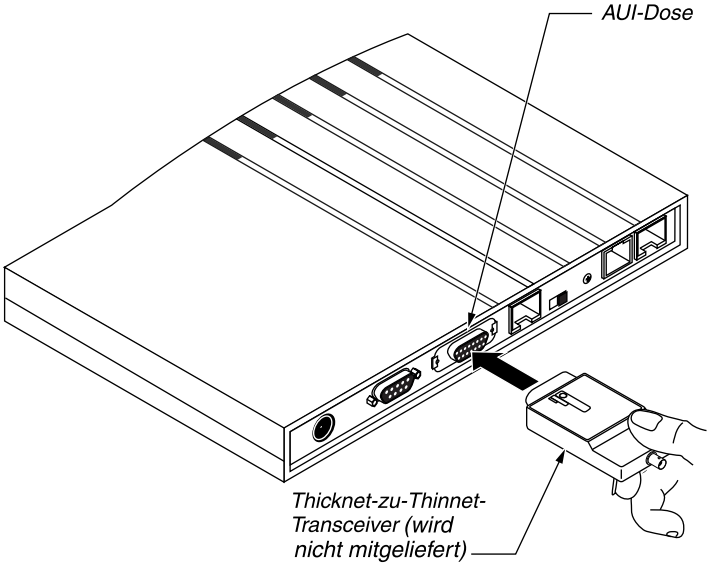


Abbildung 2-7: Anschließen des Thicknet-zu-Thinnet-Transceivers

2 Schließen Sie ein T-Verbindungsstück an den Transceiver an, und schließen Sie die Pipeline mit einem Terminator (Abschlußwiderstand) ab, falls sie das letzte Gerät im Netzwerk ist.

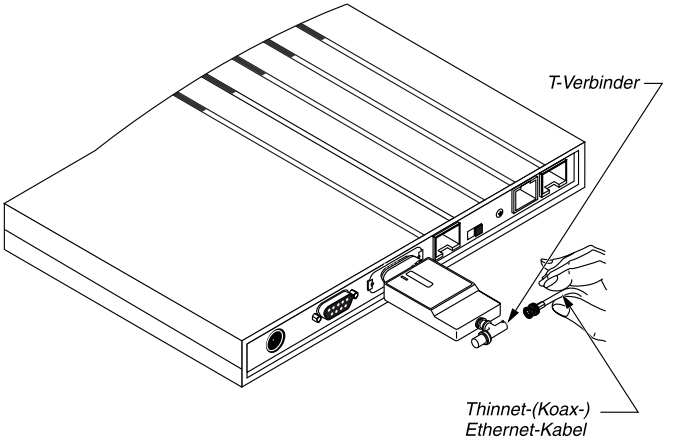


Abbildung 2-8: Anschließen des T-Verbindungsstücks und Terminators an den Transceiver

3 Schließen Sie das Thinnet-Koaxkabel an das T-Verbindungsstück an.

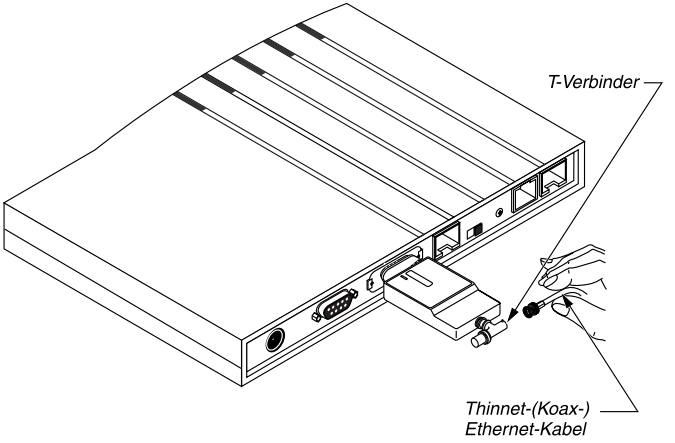


Abbildung 2-9: Anschließen des Thinnet-Kabels

4 Besorgen Sie sich ein T-Verbindungsstück für das andere Ende des Kabels.

Ist der Computer am anderen Ende des Kabels das letzte Gerät an diesem Ende des Netzwerks, muß er mit einem Terminator (Abschlußwiderstand) versehen werden.

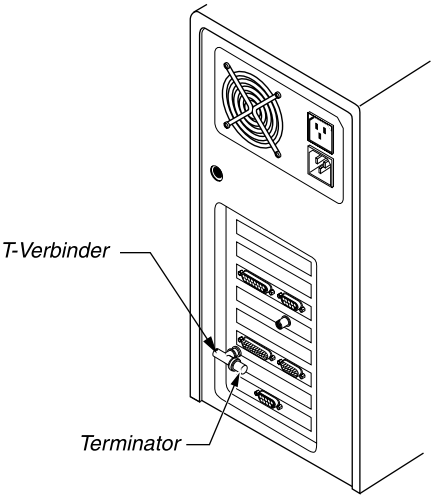


Abbildung 2-10: Anschließen eines zweiten T-Stücks und Terminators

5 Verbinden Sie das andere Ende des Kabels mit dem T-Verbindungsstück, und schließen Sie das T-Verbindungsstück an die Ethernet-Schnittstelle des Computers an.

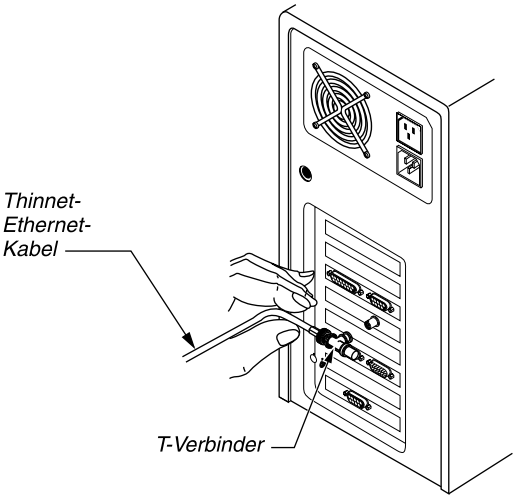


Abbildung 2-11: Anschließen des Thinnet-Kabels an das T-Verbindungsstück

Wie geht's weiter?

- Fahren Sie mit den Anweisungen im Abschnitt „Anschließen eines Computers an den Terminal-Anschluß der Pipeline“ auf Seite 2-17 fort.

Anschließen eines Computers an den Terminal-Anschluß der Pipeline

Zur Konfiguration der Pipeline (siehe nächstes Kapitel) verwenden Sie einen Computer und eine serielle Schnittstelle (COM-Schnittstelle). In den folgenden Abschnitten wird erklärt, wie Sie verschiedene Computerarten mit der Pipeline verbinden können:

- Soll die Pipeline mit einem IBM-kompatiblen PC konfiguriert werden, siehe „Anschließen eines IBM-kompatiblen Computers“ auf Seite 2-17.
- Soll die Pipeline mit einem Macintosh-Computer konfiguriert werden, siehe „Anschließen eines Macintosh-Computers“ auf Seite 2-18.
- Soll die Pipeline mit einer Unix-Workstation konfiguriert werden, siehe „Anschließen einer Unix-Workstation“ auf Seite 2-20.

Anschließen eines IBM-kompatiblen Computers

Zum Anschließen eines IBM-kompatiblen PCs an die Pipeline gehen Sie wie folgt vor:

1 Suchen Sie einen freien seriellen Anschluß an Ihrem Computer.

Notieren Sie sich die Nummer des seriellen Anschlusses, mit dem die Pipeline verbunden werden soll (meistens COM1 oder COM2). Diese Angabe benötigen Sie später bei der Einrichtung der Konfigurationssoftware. Sind alle seriellen Anschlüsse Ihres Computers belegt, müssen Sie eines der Geräte, das einen seriellen Anschluß benutzt (z. B. ein externes Modem), vorübergehend von diesem Anschluß trennen.

2 Schließen Sie ein Modemkabel an den seriellen Anschluß an.

3 Wenn der Stecker am anderen Ende des Modemkabels 25polig ist, muß der mitgelieferte Adapter (25polig-zu-9polig, Teile-Nr. 2510-0052-002) aufgesteckt werden.

4 Schließen Sie das Kabel an den Terminal-Anschluß an der Rückseite der Pipeline an.

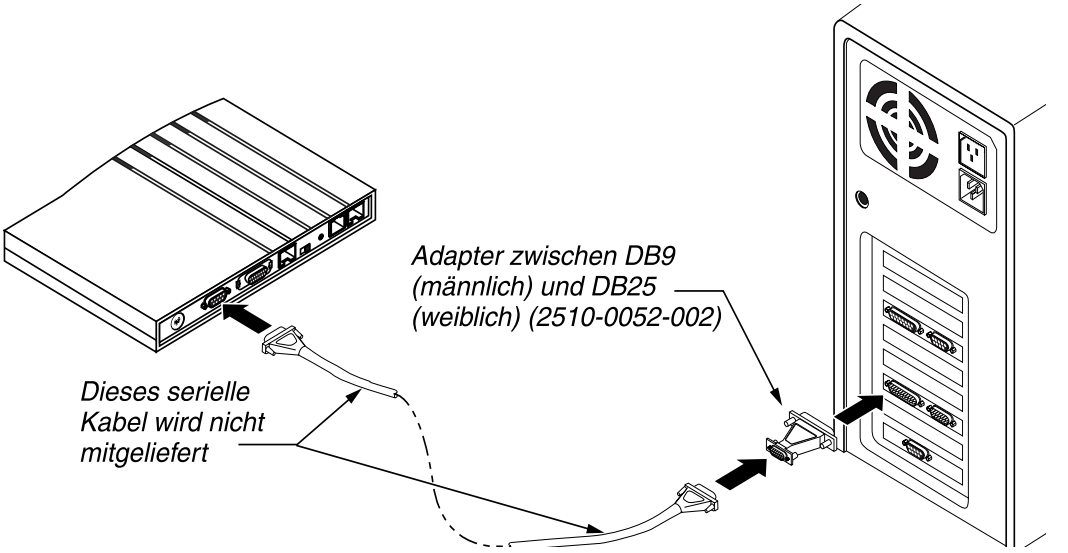


Abbildung 2-12: Anschließen des Modemkabels an den Terminal-Anschluß der Pipeline

Wie geht's weiter?

- Wenn Sie die Pipeline mit einer Mietleitung verbinden wollen, fahren Sie mit „Anschließen der Pipeline an eine Mietleitung“ auf Seite 2-21 fort.
- Wenn Sie die Pipeline nicht mit einer Mietleitung verbinden wollen, fahren Sie mit „Starten der Pipeline“ auf Seite 2-22 fort.

Anschließen eines Macintosh-Computers

Zum Anschließen eines Macintosh-Computers (oder eines kompatiblen Computers) an die Pipeline gehen Sie wie folgt vor:

1 Schließen Sie den mitgelieferten Adapter (25polig-zu-9polig, Teile-Nr. 2510-0052-002) an das DB-25-Ende eines Macintosh-Modemkabels an.

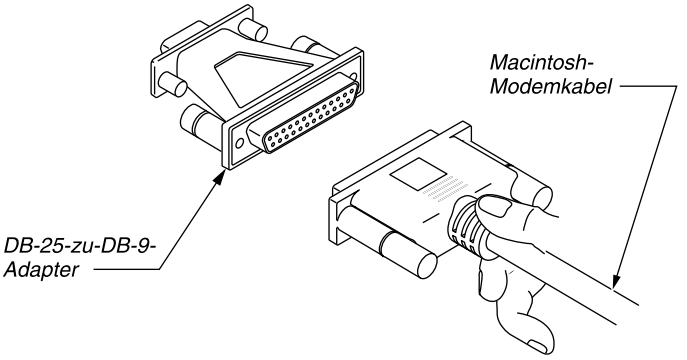


Abbildung 2-13: Anschließen des Adapters an ein Macintosh-Modemkabel

2 Schließen Sie das Kabel an den Terminal-Anschluß an der Rückseite der Pipeline an.

3 Schließen Sie das andere Ende des Kabels an einen seriellen Anschluß des Computers an (entweder der Modem- oder der Druckeranschluß).

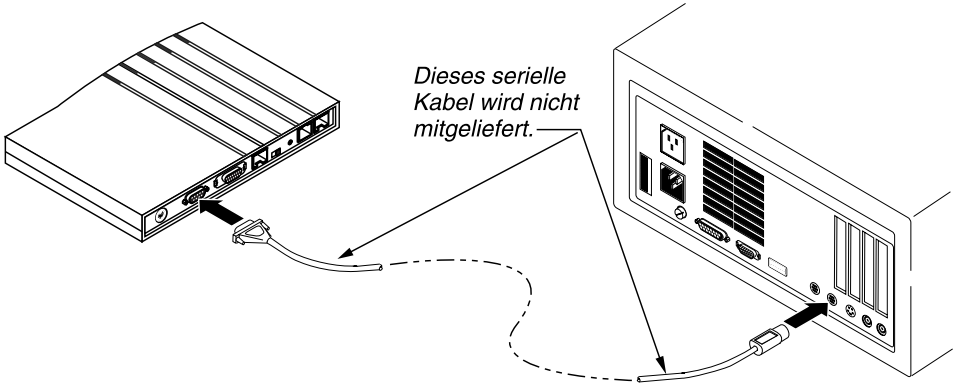


Abbildung 2-14: Anschließen eines Macintosh-Computers an den Terminal-Anschluß der Pipeline

Wie geht's weiter?

- Wenn Sie die Pipeline mit einer Mietleitung verbinden wollen, fahren Sie mit „Anschließen der Pipeline an eine Mietleitung“ auf Seite 2-21 fort.
- Wenn Sie die Pipeline nicht mit einer Mietleitung verbinden wollen, fahren Sie mit „Starten der Pipeline“ auf Seite 2-22 fort.

Anschließen einer Unix-Workstation

Zum Anschließen einer Unix-Workstation bzw. eines anderen Computers, auf dem Unix läuft, gehen Sie wie folgt vor:

1 Schließen Sie das eine Ende eines Modemkabels an den Terminal-Anschluß auf der Rückseite der Pipeline an.

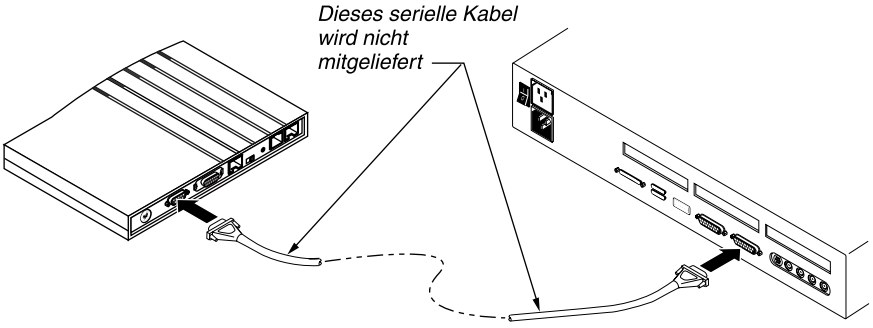


Abbildung 2-15: Anschließen des Modemkabels an den Terminal-Anschluß der Pipeline

2 Schließen Sie das andere Ende des Kabels an den seriellen Anschluß des Computers an.

Wie geht's weiter?

- Wenn Sie die Pipeline mit einer Mietleitung verbinden wollen, fahren Sie mit „Anschließen der Pipeline an eine Mietleitung“ auf Seite 2-21 fort.
- Wenn Sie die Pipeline nicht mit einer Mietleitung verbinden wollen, fahren Sie mit „Starten der Pipeline“ auf Seite 2-22 fort.

Anschließen der Pipeline an eine Mietleitung

Wenn Sie Ihre Pipeline an eine Mietleitung anschließen wollen, sollten Sie sich diesen Abschnitt durchlesen, bevor Sie beginnen, die Einheit zu konfigurieren.

Achtung: Um Störungen des WAN-Betriebs zu vermeiden, müssen Sie vor der Installation der Pipeline an die Mietleitung eine Genehmigung des WAN-Betreibers einholen. Wenn Sie die Pipeline wieder vom WAN trennen möchten, ist der WAN-Betreiber davon in Kenntnis zu setzen. Wird die Pipeline ohne vorherige Ankündigung vom WAN getrennt oder ausgeschaltet, kann dies zu einer vorübergehenden Abschaltung Ihrer Mietleitung durch den WAN-Betreiber führen.

Zum Anschluß der Pipeline an eine Mietleitung ist wie folgt vorzugehen:

1. Verbinden Sie Ihre Mietleitungen mit dem entsprechenden WAN-Anschluß der Pipeline. Schließen Sie das andere Ende direkt oder über andere Netzwerkschnittstelleneinrichtungen an die Mietleitung an.
2. Informieren Sie Ihren WAN-Betreiber, daß Ihr Gerät angeschlossen ist, damit dieser die Leitung aufbauen kann.

Nachdem Sie nun die Pipeline an Ihr WAN angeschlossen haben, können Sie die Einheit starten.

Hinweis: Bevor Sie die Mietleitung verwenden können, müssen Sie sie zunächst konfigurieren. Siehe dazu Kapitel 5, „Konfigurieren von WAN-Verbindungen“.

Wie geht’s weiter?

- Siehe „Starten der Pipeline“ auf Seite 2-22.

Starten der Pipeline

Zum Starten der Pipeline ist wie folgt vorzugehen:

1 Starten Sie das DFÜ-Programm auf Ihrem Computer.

2 Legen Sie in Ihrem DFÜ-Programm die folgenden Einstellungen für die Terminal-Emulation fest:

- VT100-Emulation
- 9600 Bits pro Sekunde (bps)
- 8 Datenbits
- keine Parität
- 1 Stoppbit
- keine Flußkontrolle
- Direktverbindung

3 Begeben Sie sich in eine Position, von der aus Sie sowohl die LED-Anzeigen an der Frontblende als auch die VT100-Anzeige sehen können.

Warnung: Die folgenden Schritte sind **unbedingt in der angegebenen Reihenfolge** auszuführen! Das Anschließen des Netzteils an das Stromnetz, ohne es zuvor mit der Pipeline verbunden zu haben, kann zu Funkenflug, Feuer oder zur Zerstörung der Pipeline führen.

4 Stecken Sie das Stromkabel in den Netzanschluß der Pipeline.

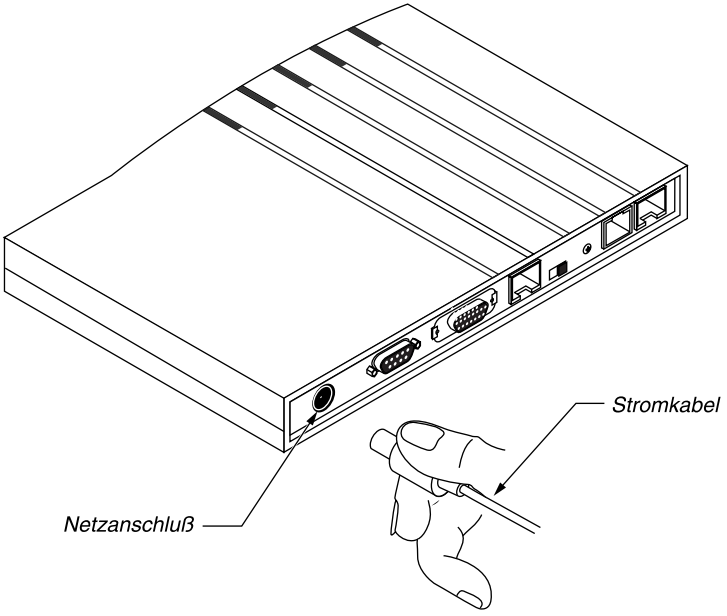


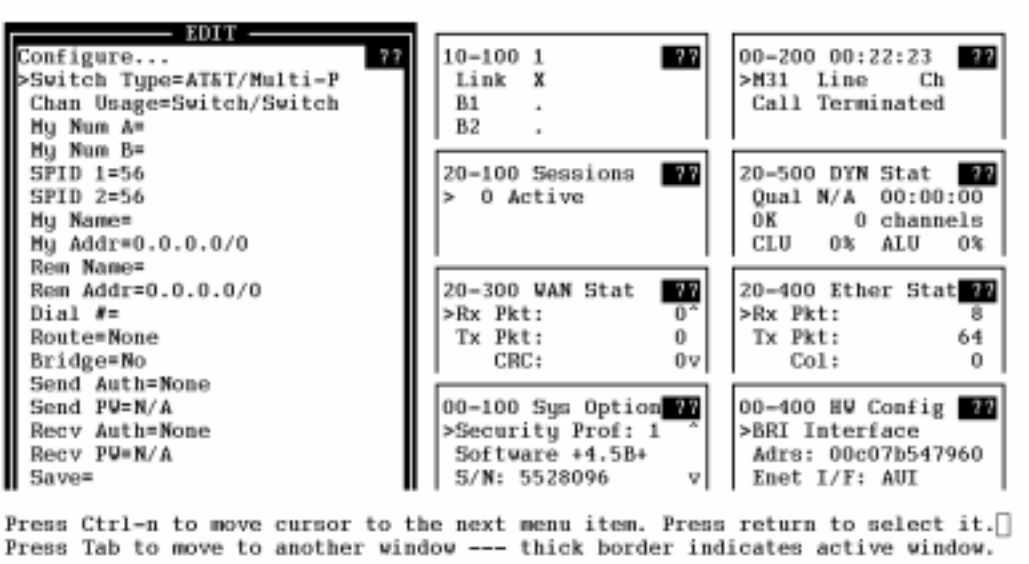
Abbildung 2-16: Anschließen des Stromkabels an die Pipeline

5 Stecken Sie die andere Seite des Stromkabels (Wechselstromstecker) in die Netzsteckdose.

Die Pipeline verfügt über keinen eigenen Netzschalter, so daß sie durch das Anschließen an das Netz eingeschaltet wird. Nach dem Anschließen der Pipeline an das Stromnetz dauert es ungefähr eine Minute, bis sie einsatzbereit ist. Sobald die Verbindung zum Stromnetz hergestellt ist, leuchtet die LED „PWR“ an der Frontblende der Pipeline auf, um anzuzeigen, daß die Pipeline eingeschaltet ist.

Die LED „CON“ beginnt zu leuchten, wenn Sie die Pipeline an das Stromnetz anschließen, und erlischt, sobald die internen Selbsttests nach dem Einschalten (Power-on Self Tests, POSTs) erfolgreich abgeschlossen wurden.

Die POSTs dauern ca. eine Minute. Wurde der POST erfolgreich abgeschlossen, wird auf dem Bildschirm folgendes angezeigt (die genauen Werte hängen von der jeweiligen Konfiguration ab):



Erscheint diese Anzeige nicht, können Sie folgendes versuchen:

- Drücken Sie die Tastenkombination Strg-L, um die Bildschirmanzeige zu aktualisieren.
- Kontrollieren Sie, daß das serielle Kabel sowohl an der Pipeline als auch am Computer ordnungsgemäß befestigt ist.
- Kontrollieren Sie, daß die Einstellungen Ihres DFÜ-Programms den Angaben auf Seite 2-21 entsprechen.

Kann das Problem auf diese Weise nicht behoben werden, können Sie im Appendix B, “Fehlersuche und -beseitigung.” ausführliche Informationen zur Fehlerbeseitigung finden.

Wie geht’s weiter?

- Wenn Sie sich eine Übersicht über die Bedeutung der einzelnen LED-Anzeigen ansehen wollen, lesen Sie den Abschnitt „Bedeutung der Pipeline-LEDs“ auf Seite 2-26.
- Wenn Sie die Pipeline an einer Wand anbringen möchten, lesen Sie den Abschnitt „Wandmontage der Pipeline“ auf Seite 2-27.
- Wenn Sie die Pipeline konfigurieren möchten, lesen Sie Kapitel 3, „Pipeline-Grundeinstellungen“ In diesem Kapitel wird erläutert, wie Sie die grundlegenden Konfigurationseinstellungen für Ihre Pipeline festlegen können.

Bedeutung der Pipeline-LEDs

Abbildung 2-17 zeigt die Bedeutung der LEDs an der Frontblende der Pipeline.

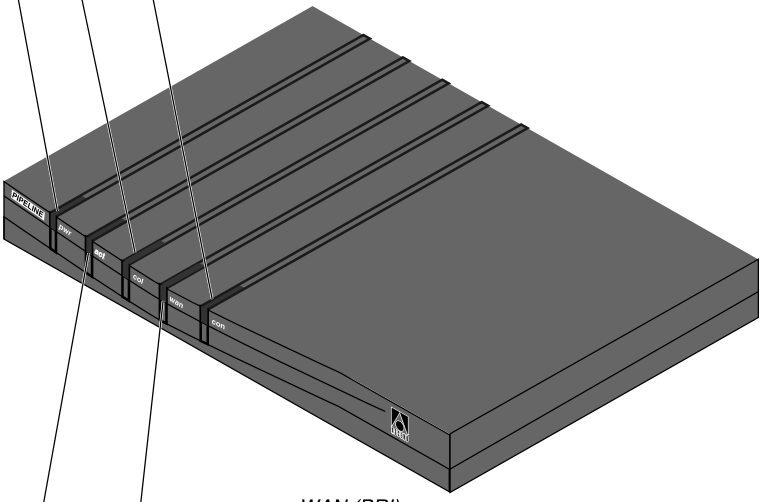


Abbildung 2-17: LEDs an der Frontblende der Pipeline

Wandmontage der Pipeline

In einigen Fällen ist es sinnvoll, die Pipeline an einer Wand zu montieren, statt sie auf einer flachen Unterlage aufzustellen. An der Unterseite der Pipeline befinden sich zu diesem Zweck zwei Montagelöcher. Aus der folgenden Abbildung können Sie entnehmen, was für Schrauben Sie für die Wandmontage benötigen und wie die Löcher zu bohren sind.

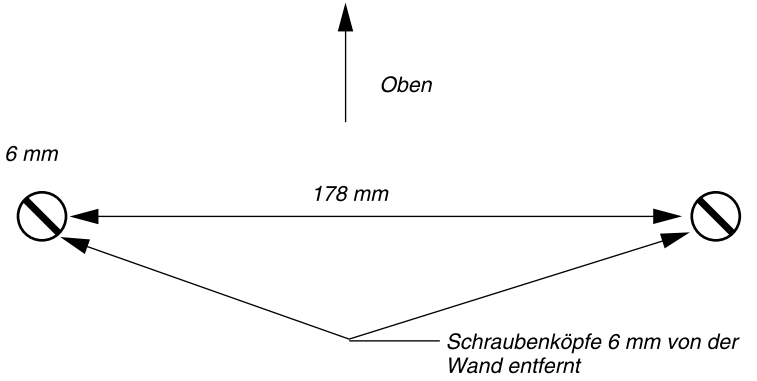


Abbildung 2-18: Position der Schrauben für die Wandmontage der Pipeline

Wie geht's weiter?

- Siehe Kapitel 3, „Pipeline-Grundeinstellungen“ In diesem Kapitel wird erläutert, wie Sie die grundlegenden Konfigurationseinstellungen für Ihre Pipeline festlegen können.

Pipeline-Grundeinstellungen

3

In diesem Kapitel wird erklärt, wie Sie die Grundeinstellungen für Ihre Pipeline-WAN-Schnittstelle und die Parameter für das entfernte Netzwerk festlegen können.

Das Kapitel enthält die folgenden Abschnitte:

Einführung

In diesem Kapitel wird die Vorgehensweise zur Konfiguration einer einzelnen Verbindung zu einem entfernten Netzwerk sowie zur Festlegung der grundlegenden Pipeline-Parameter erläutert. Ziel des Kapitels ist es, Sie in die Lage zu versetzen, die Pipeline, wenn möglich, mit den Grundeinstellungen zu betreiben.

Weitergehende Einstellungen werden weiter hinten in diesem Handbuch beschrieben. Hinweise zur Konfiguration von Frame-Relay-Verbindungen können Sie dem Abschnitt „Konfigurieren von Frame-Relay-Verbindungen“ auf Seite 5-26 entnehmen.

Für eine erfolgreiche Konfiguration Ihrer Pipeline benötigen Sie Informationen sowohl von Ihrem WAN-Diensteanbieter als auch vom Administrator des entfernten Netzwerks. Dieses Kapitel enthält Konfigurationsarbeitsblätter, die Ihnen helfen sollen, die erforderlichen Informationen zu erhalten.

Die Konfiguration der Pipeline umfaßt die folgenden Schritte:

1 Einholen von Informationen über Ihre WAN-Schnittstelle

2 Einholen der Informationen, die Sie für den Zugriff auf das entfernte Netzwerk benötigen

3 Festlegen bestimmter Einstellungen für Ihren Computer, so daß dieser der Pipeline-Konfiguration und der Konfiguration des entfernten Netzwerks entspricht

4 Eingeben der Informationen zur WAN-Schnittstelle und zum entfernten Netzwerk

5 Testen des Anschlusses

6 Herstellen einer Testverbindung mit dem entfernten Netzwerk

Miet- und Wählleitungen

Je nachdem, was für ein Pipeline-Modell Sie haben, stehen Ihnen entweder Funktionen für Mietleitungen (auch „festgeschaltete Leitungen“ oder „Standleitungen“ genannt) oder aber Funktionen für Wählleitungen („vermittelte Leitungen“) zur Verfügung.

Eine Mietleitung ist eine permanente Verbindung zwischen zwei Geräten.

Eine Wählleitung ist eine temporäre Verbindung zwischen zwei Geräten, die durch das Aufhängen auf einer der beiden Seiten beendet wird. Ein Beispiel für Wählleitungen sind z. B. normale Telefonanrufe.

Die Konfiguration der Pipeline hängt von den jeweiligen Verkehrserfordernissen ab. Wenn Sie bei Ihrem WAN-Diensteanbieter eine Standleitung mieten, wird diese Leitung als Ihre primäre Verbindung konfiguriert. Als Backup-Leitung oder zweite Leitung kann dann eine Wählleitung (z. B. eine ISDN-Leitung) verwendet werden, sollte die Mietleitung einmal ausfallen oder nicht verfügbar sein.

Sie können die Mietleitung auch als primäre Verbindung konfigurieren und die Wählleitungen als alternative Verbindungen für das Einwählen in andere LANs oder in das Internet verwenden.

In diesem Kapitel wird beschrieben, wie Sie eine Wählleitung (vermittelte Leitung) als erstes Verbindungsprofil (mit Hilfe des „Configure“-Profils) und die Mietleitung als zweites Verbindungsprofil konfigurieren können. Dies ist bei weitem nicht die einzige Möglichkeit, Ihre Pipeline zu konfigurieren. Informationen zur Konfiguration anderer WAN-Verbindungstypen (z. B. Frame-Relay-Verbindungen oder Verbindungen über die serielle WAN-Schnittstelle) finden Sie im Kapitel 5, „Konfigurieren von WAN-Verbindungen“.

Erforderliche Informationen zum ISDN-Anschluß

Hinweis: Die neuesten Informationen zur Bereitstellung von ISDN-Anschlüssen erfahren Sie unter der WWW-Adresse von Ascend (www.ascend.com).

Hinweis: Ausführliche Informationen zu diesen Parametern können Sie dem *Referenzhandbuch* entnehmen.

Tabelle 3-1: Informationen zum ISDN-Anschluß

Parameter	Standardwert	Meine Konfiguration	Anmerkungen
„Configure“-Profil > Switch Type	NET 3		ISDN-Switchtyp für EURO-ISDN
„Configure“-Profil > **Chan Usage**	Switch/Switch		Nutzung der ISDN-B-Kanäle
„Configure“-Profil > **My Num A**	555-5551212		Telefonnummer des ersten ISDN-B-Kanals
„Configure“-Profil > **My Num B**	555-5551213		Telefonnummer des zweiten ISDN-B-Kanals
„Configure“-Profil > **SPID 1**	N/A		SPID für „My Num A“ für EURO-ISDN nicht erforderlich
„Configure“-Profil > **SPID 2**	N/A		SPID für „My Num B“ für EURO-ISDN nicht erforderlich

Erforderliche IP-Informationen

Diese Informationen, die Sie von Ihrem Netzwerkadministrator erhalten, werden für den Zugriff auf ein entferntes IP-Netzwerk benötigt. Die Pipeline nutzt diese Informationen zur Erstellung des ersten Verbindungsprofils.

Tabelle 3-2: Informationen zum entfernten IP-Netzwerk

Parameter	Standardwert	Meine Konfiguration	Anmerkungen
„Configure“-Profil > **My Name**			Name Ihrer Pipeline
„Configure“-Profil > **My Addr**	0.0.0.0/0		IP-Adresse Ihrer Pipeline; normalerweise fungiert diese Adresse als Gateway für Ihren Computer
„Configure“-Profil > **Rem Name**			Name des entfernten Geräts
„Configure“-Profil > **Rem Addr**	0.0.0.0/0		IP-Adresse des entfernten Geräts; dieser Wert wird zur Erstellung der Standardroute verwendet
„Configure“-Profil > **Dial #**			Telefonnummer für die Einwahl in das entfernte Netzwerk
„Configure“-Profil > **Route**	None		Art des Routings: IP, IPX oder beides
„Configure“-Profil > **Bridge**	Yes		Bridging ja oder nein

Tabelle 3-2: Informationen zum entfernten IP-Netzwerk (Fortsetzung)

Parameter	**Standardwert**	**Meine Konfiguration**	**Anmerkungen**
„Configure“-Profil > **Send Auth**	None		Für das entfernte Netzwerk erforderliche Authentifizierung
„Configure“-Profil > **Send PW**	N/A		Für das entfernte Netzwerk erforderliches Kennwort
„Configure“-Profil> **Recv Auth**	None		Authentifizierung für Ihre Pipeline
„Configure“-Profil > **Recv PW**	N/A		Kennwort für ankommende Rufe

Erforderliche IPX-Informationen

Diese Informationen, die Sie von Ihrem Netzwerkadministrator erhalten, werden für den Zugriff auf das entfernte Novell-NetWare-Netzwerk benötigt.

Tabelle 3-3: Informationen über das entfernte IPX-Netzwerk

Parameter	Standardwert	Meine Konfiguration	Anmerkungen
„Configure“-Profil > **My Name**			Name Ihrer Pipeline
„Configure“-Profil > **Rem Name**			Name des entfernten Geräts
„Configure“-Profil > **Dial #**			Telefonnummer für die Einwahl in das entfernte Netzwerk
„Configure“-Profil > **Send Auth**	None		Für das entfernte Netzwerk erforderliche Authentifizierung
„Configure“-Profil > **Send PW**	N/A		Für das entfernte Netzwerk erforderliches Kennwort
„Configure“-Profil > **Recv Auth**	None		Authentifizierung für Ihre Pipeline
„Configure“-Profil > **Recv PW**	N/A		Kennwort für ankommende Rufe
„Configure“-Profil > **Bridge**	Yes		Bridging ja oder nein
„Configure“-Profil > **Route**	None		Art des Routings: IP, IPX oder beides

Tabelle 3-3: Informationen über das entfernte IPX-Netzwerk

Parameter	Standardwert	Meine Konfiguration	Anmerkungen
Ethernet > Mod Config > Ether options > **IPX Frame**	None		Ethernet-Rahmentyp für IPX im Ethernet
Ethernet > Mod Config > Ether options > **IPX Enet#**	00000000		Eindeutige IPX-Netzwerknummer für die Ethernet-Schnittstelle. Wenn Sie die Standardeinstellung verwenden („00000000“), „lernt“ die Pipeline ihre IPX-Netzwerknummer von anderen Routern im Netzwerk.
Ethernet > Mod Config > Ether options > **IPX SAP Proxy**	No		IPX-SAP-Proxy-Modus der Pipeline aktiviert oder deaktiviert
Ethernet > Mod Config > Ether options > **IPX SAP Proxy Net#**	00000000		IPX-Netzwerknummer des Geräts am anderen Ende der WAN-Verbindung
Ethernet > Mod Config > Ether options > **Dial Query**	No		Gibt an, ob die Pipeline einen Ruf an den im Verbindungsprofil angegebenen Ort initiiert, wenn eine Workstation im lokalen IPX-Netzwerk nach dem nächsten IPX-Server sucht.

Konfiguration des Computers

Für die Verbindung mit einem IP-Netzwerk mit Hilfe der Pipeline müssen auf Ihrem Computer die folgenden Einstellungen vorgenommen werden:

- Als Standard-Gateway für Ihren Computer muß die Pipeline festgelegt werden (nur bei IP und AppleTalk).
- Die IP-Adresse Ihres Computers muß so festgelegt werden, daß sich Ihr Computer im selben IP-Subnetz wie die Pipeline befindet (nur bei IP und AppleTalk).
- Auf Ihrem Computer muß das Domänennamensystem (DNS) eingestellt werden, das vom entfernten Netzwerk benutzt wird (nur bei IP und AppleTalk).

Diese Einstellungen sind notwendig, damit Ihr Computer ordnungsgemäß mit der Pipeline und dem entfernten Netzwerk kommunizieren kann.

Eingeben der ISDN-Parameter

Die von Ihnen eingeholten ISDN-Informationen müssen in das „Configure“-Profil eingegeben werden.

Hinweis: Welche Parameter im „Configure“-Profil festgelegt werden müssen, hängt davon, was für einen ISDN-Anschluß Sie haben. Die nicht benötigten Parameter haben den Wert „N/A“. In diese Felder muß nichts eingetragen werden.

Zur Eingabe der ISDN-Parameter ist wie folgt vorzugehen:

1 Öffnen Sie das „Configure“-Profil.

Falls erforderlich, drücken Sie die Esc-Taste, bis das „Main Edit Menu“ erscheint. Markieren Sie dann die Option „Configure“, und drücken Sie die Eingabetaste.

Es erscheint das „Configure“-Profil.

```
Configure..
>Switch Type=AT&T/Multi-P
 Chan Usage=Switch/Switch
 My Num A=
 My Num B=
 SPID 1=
 SPID 2=
 Data Usage=A+B
 Phone 1 Usage=A
 Phone 2 Usage=B
 Phone Num Binding=N/A
 My Name=
 My Addr=0.0.0.0/0
 Rem Name=
 Rem Addr=0.0.0.0/0
 Dial#=
 Route=None
 Bridge=Yes
 Send Auth=None
 Send PW=N/A
 Recv Auth=None
 Recv PW=N/A
 Save=
```

2 Markieren Sie die Option „Switch Type“.

3 Drücken Sie die Eingabetaste, bis der Switch-Typ für Ihren ISDN-Anschluß angezeigt wird.

Beachten Sie, daß bei bestimmten Switchtypen einige der Parameter nicht verfügbar sind (N/A). Diese Parameter werden für den jeweiligen Switchtyp nicht benötigt.

4 Geben Sie den für Ihren ISDN-Anschluß zutreffenden Wert für den Parameter „Chan Usage“ ein.

5 Geben Sie die Telefonnummer für Ihren ersten ISDN-B-Kanal in das Feld „My Num A“ ein.

Drücken Sie die Eingabetaste. Es erscheint ein Textfeld, in das Sie die Telefonnummer eingeben können. Drücken Sie die Eingabetaste erneut, um den Wert wirksam werden zu lassen.

Ob die restlichen Einstellungen vorgenommen werden müssen, hängt von der Art Ihres ISDN-Anschlusses ab.

6 Geben Sie die Telefonnummer für Ihren zweiten ISDN-B-Kanal in das Feld „My Num B“ ein.

7 Geben Sie die SPID für Ihren ersten ISDN-B-Kanal in das Feld „SPID 1“ ein.

8 Geben Sie die SPID für Ihren zweiten ISDN-B-Kanal in das Feld „SPID 2“ ein.

Als nächstes müssen die Parameter für das entfernte Netzwerk konfiguriert werden:

- Handelt es sich bei dem entfernten Netzwerk um ein IP-Netzwerk, gelten die Angaben im Abschnitt „Eingeben der IP-Parameter“ auf Seite 3-12.
- Handelt es sich bei dem entfernten Netzwerk um ein IPX-Netzwerk, gelten die Angaben im Abschnitt „Eingeben der IPX-Parameter“ auf Seite 3-13.

Eingeben der IP-Parameter

Zur Festlegung der Werte der grundlegenden IP-Parameter für die Pipeline und das entfernte Netzwerk ist wie folgt vorzugehen:

1 Geben Sie im „Configure“-Profil den Namen Ihrer Pipeline ein (Feld „My Name“).

2 Geben Sie im Feld „Rem Name“ den Namen des entfernten Geräts an, mit dem eine Verbindung hergestellt werden soll.

Die Pipeline verwendet diesen Namen zur Benennung des ersten Verbindungsprofils.

3 Geben Sie im Feld „Dial #“ die Telefonnummer für die Einwahl in das entfernte Netzwerk an.

4 Geben Sie im Feld „Route“ die gewünschten IP- und IPX-Routing-Optionen an (falls erforderlich).

Die Pipeline kann sowohl IP- als auch IPX-Routing durchführen.

Ob die übrigen Einstellungen benötigt werden, hängt von der jeweiligen Netzwerkkonfiguration ab.

5 Geben Sie im Feld „Bridge“ die gewünschte Bridging-Option an.

6 Geben Sie im Feld „Send Auth“ die Art der Authentifizierung an, die im entfernten Netzwerk verwendet wird.

7 Geben Sie im Feld „Send PW“ das Kennwort für das entfernte Netzwerk ein.

8 Geben Sie im Feld „Recv Auth“ die Art der Authentifizierung ein, die im lokalen Netzwerk verwendet wird.

9 Geben Sie im Feld „Recv PW“ das Kennwort ein, mit dem entfernten Geräten Zugriff auf das lokale Netzwerk gewährt wird.

10 Markieren Sie die Option „Save“, und drücken Sie dann die Eingabetaste. Ihre Änderungen werden gespeichert.

Nachdem Sie die Einstellungen im „Configure“-Profil vorgenommen haben, können Sie das ordnungsgemäße Funktionieren Ihres ISDN-Anschlusses testen. Siehe dazu „Durchführung eines Selbsttests (ISDN)“ auf Seite 3-15.

Eingeben der IPX-Parameter

Zur Festlegung der Werte der grundlegenden IPX-Parameter für die Pipeline und das entfernte Netzwerk ist wie folgt vorzugehen:

1 Geben Sie im „Configure“-Profil den Namen Ihrer Pipeline ein (Feld „My Name“).

2 Geben Sie im Feld „Rem Name“ den Namen des entfernten Geräts an, mit dem eine Verbindung hergestellt werden soll.

Die Pipeline verwendet diesen Namen zur Benennung des ersten Verbindungsprofils.

3 Geben Sie im Feld „Dial #“ die Telefonnummer für die Einwahl in das entfernte Netzwerk an.

4 Geben Sie im Feld „Route“ die gewünschten IP- und IPX-Routing-Optionen an (falls erforderlich).

Ob die übrigen Einstellungen benötigt werden, hängt von der jeweiligen Netzwerkkonfiguration ab.

5 Geben Sie im Feld „Bridge“ die gewünschte Bridging-Option an.

6 Geben Sie im Feld „Send Auth“ die Art der Authentifizierung an, die im entfernten Netzwerk verwendet wird.

7 Geben Sie im Feld „Send PW“ das Kennwort für das entfernte Netzwerk ein.

8 Geben Sie im Feld „Recv Auth“ die Art der Authentifizierung ein, die im lokalen Netzwerk verwendet wird.

9 Geben Sie im Feld „Recv PW“ das Kennwort ein, mit dem entfernten Geräten Zugriff auf das lokale Netzwerk gewährt wird.

10 Markieren Sie die Option „Save“, und drücken Sie dann die Eingabetaste. Ihre Änderungen werden gespeichert.

Als nächstes müssen die IPX-Parameterwerte festgelegt werden.

11 Öffnen Sie das Untermenü „Ethernet“ > „Mod Config“ > „Ether options“.

```
Ether options...
IP Adrs
2nd Adrs
RIP
Ignore Def Rt
Proxy Mode
Filter
IPX Frame
IPX Enet#
IPX Pool#
IPX SAP Filter
IPX SAP Proxy
IPX SAP Proxy Net#
```

12 Geben Sie den IPX-Rahmentyp an (Feld „IPX Frame“).

13 Geben Sie die IPX-Ethernet-Netzwerknummer an (Feld „IPX Enet#“).

14 Geben Sie die IPX-Pool-Nummer an (Feld „IPX Pool#“).

15 Aktivieren bzw. deaktivieren Sie den IPX-SAP-Proxy-Modus (Feld „IPX SAP Proxy“).

16 Geben Sie die IPX-SAP-Proxy-Netzwerknummer an (Feld „IPX SAP Proxy Net#“).

Nachdem Sie die IPX-Angaben eingegeben haben, können Sie das ordnungsgemäße Funktionieren Ihres ISDN-Anschlusses testen.

Überprüfen des Anschlußstatus und der Verbindung zum entfernten Netzwerk

Nachdem Sie alle Informationen zum Anschluß und zum entfernten Netzwerk eingegeben haben, können Sie überprüfen, ob eine Verbindung zum entfernten Netzwerk hergestellt werden kann.

In diesem Abschnitt wird erklärt, wie Sie den Leitungsstatus und die Möglichkeit einer Verbindung zum entfernten Netzwerk für ISDN-Anschlüsse und für V.35-Anschlüsse überprüfen können.

Durchführung eines Selbsttests (ISDN)

Nach der Eingabe der Parameterwerte für den ISDN-Anschluß und das entfernte Netzwerk können Sie einen Selbsttest durchführen lassen, um das ordnungsgemäße Funktionieren des ISDN-Anschlusses und der Pipeline-Konfiguration zu überprüfen. Dies geschieht mit Hilfe der Pipeline-Terminal-Server-Schnittstelle (siehe unten). Ausführliche Informationen zur Arbeit mit der Terminal-Server-Schnittstelle finden Sie im Kapitel 11, „Systemadministration“.

Zur Durchführung eines Selbsttests ist wie folgt vorzugehen:

1 Markieren Sie im „Main Edit Menu“ die Option „System“.

2 Drücken Sie die Eingabetaste.

3 Wählen Sie „Sys Diag“.

4 Wählen Sie „Term Serv“.

5 Drücken Sie die Eingabetaste.

Es erscheint die Ascend-Pipeline-Terminal-Server-Schnittstelle.

Geben Sie am `ascend%`-Prompt den Befehl **`test [My Num]`** ein.

Dabei gilt folgendes:

- [My Num] ist die Nummer, die Sie im Feld „My Num A“ eingegeben haben (falls Ihr ISDN-Anschluß nur mit einer Telefonnummer ausgestattet ist), bzw.
- [My Num] ist die Nummer, die Sie im Feld „My Num B“ eingegeben haben (falls Ihr ISDN-Anschluß mit zwei Telefonnummern ausgestattet ist).

Die Pipeline zeigt den gegenwärtigen Status des Rufes an. Wenn der ISDN-Anschluß richtig konfiguriert wurde, erscheint die folgenden Meldung:

```
calling...answering...testing...end
100 packets sent, 100 packets received
```

6 War der Test erfolgreich, können Sie durch Eingabe des Befehls **`quit`** am `ascend%`-Prompt zur Konfigurationsschnittstelle zurückkehren.

- Wenn der Test erfolgreich abgeschlossen wurde, befolgen Sie die Anweisungen im nächsten Abschnitt, um sich in das entfernte Netzwerk einzuwählen und zu überprüfen, ob die Parameter für das entfernte Netzwerk ordnungsgemäß festgelegt wurden.

- Wenn der Test nicht erfolgreich abgeschlossen werden konnte, ist zu überprüfen, ob auch wirklich die richtige Telefonnummer eingegeben wurde. Bestehen die Probleme weiter, finden Sie im Anhang B, „Fehlersuche und -beseitigung“, entsprechende Informationen zur Fehlersuche und -beseitigung.

Einwählen in das entfernte Netzwerk (ISDN)

In diesem Abschnitt wird erläutert, wie Sie sich mit Hilfe der Parameter im „Configure“-Profil in das entfernte Netzwerk einwählen können.

1 Öffnen Sie das „Configure“-Profil.

2 Drücken Sie die Tastenkombination Strg-D.

Es erscheint das DO-Menü.

3 Wählen Sie die Option „1, Dial“.

Die Pipeline wählt einen abgehenden Ruf. Beobachten Sie die Anzeige in der rechten oberen Ecke des Statusfensters. Wenn dort die Meldung „LAN Session Up“ erscheint, wurde der Ruf erfolgreich aufgebaut.

Erscheint eine andere Meldung, ist zu überprüfen, ob alle Informationen richtig eingegeben wurden. Gelingt es Ihnen dennoch nicht, eine Verbindung herzustellen, finden Sie im Anhang B, „Fehlersuche und -beseitigung“, entsprechende Informationen zur Fehlersuche und -beseitigung.

Wenn die Pipeline erfolgreich konfiguriert wurde, stellt Sie automatisch eine Verbindung mit dem entfernten Netzwerk her, sobald sie Verkehr für dieses Netzwerk empfängt. Dies ist z. B. dann der Fall, wenn Sie einen Web-Browser öffnen, eines der Elemente in der Macintosh-Auswahl markieren oder eine E-Mail-Anwendung öffnen.

Überprüfen des Anschlußstatus (Standleitung)

Den Status der Standleitung können Sie im Fenster „10-100 Link Status“ ablesen. Erscheint dort der Wert „A“, wurde eine Verbindung hergestellt. Wenn keine Verbindung besteht, wird ein „X“ angezeigt.

Überprüfen der Verbindung zum entfernten LAN

Ob eine Verbindung mit dem entfernten LAN besteht, können Sie dem Statusfenster „00-200“ in der rechten oberen Ecke des Bildschirms entnehmen. Wenn eine Verbindung besteht, wird „LAN session up.“ angezeigt

Wie geht's weiter?

- Wenn Sie ausführliche Informationen über die Arbeit mit der Konfigurationsschnittstelle der Pipeline benötigen, lesen Sie Kapitel 4, „Die Pipeline-Benutzeroberfläche“.
- Wenn Sie Informationen zur Konfiguration Ihrer WAN-Schnittstellen benötigen, lesen Sie Kapitel 5, „Konfigurieren von WAN-Verbindungen“.

Die Pipeline-Benutzeroberfläche

4

In diesem Kapitel finden Sie die folgenden Abschnitte:

Die Konfigurationsmenüs

Die Pipeline-Konfigurationsmenüs werden in einem VT100-Emulationsfenster angezeigt, auf das Sie von einem mit dem Terminal-Anschluß verbundenen Computer aus zugreifen können. Wie Sie Ihren Computer an den Terminal-Anschluß anschließen können, erfahren Sie im Abschnitt „Anschließen eines Computers an den Terminal-Anschluß der Pipeline“ auf Seite 2-17. Sobald Sie die Konfigurationsmenüs sehen können, haben Sie eine Konsolensitzung aufgebaut.

Konsolensitzungen können von jeder Telnet-Workstation aus gestartet werden (nachdem die Pipeline für den Betrieb innerhalb des LAN konfiguriert wurde), indem Sie eine Telnet-Sitzung mit der Pipeline öffnen. Sobald Sie das Telnet-Kennwort angegeben haben, werden die Konfigurationsmenüs im Telnet-VT100-Fenster angezeigt. Von einer Telnet-Sitzung aus können alle Konfigurations-, Diagnose-, Verwaltungs- und anderen Funktionen ausgeführt werden, die von einem an den Terminal-Anschluß der Pipeline angeschlossenen Computer aus ausgeführt werden können. Siehe dazu auch „Pipeline-Kennwörter“ auf Seite 4-9.

Darüber hinaus können Sie mit dem Befehl „Rem Mgmt“ die entfernte Seite eines MPP-Rufs in die Lage versetzen, auf die Pipeline-Konfigurationsmenüs zuzugreifen.

Das Hauptbearbeitungsmenü („Main Edit Menu“)

Die Konfigurationsschnittstelle besteht aus dem Hauptbearbeitungsmenü („Main Edit Menu“) sowie acht Statusfenstern. Auf der linken Seite des Bildschirms finden Sie das „Main Edit Menu“, mit dessen Hilfe die Pipeline konfiguriert wird. Siehe Abbildung 4-1

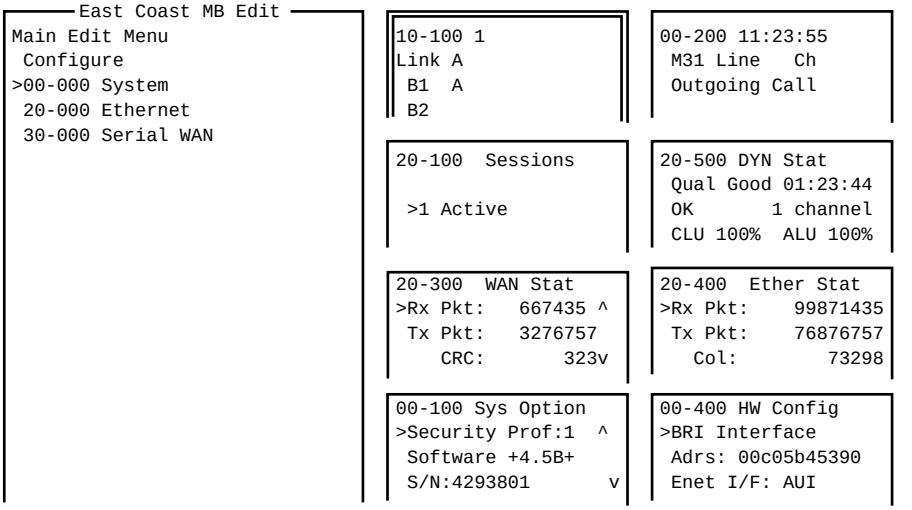


Abbildung 4-1: Die Pipeline-Konfigurationsmenüs

Organisation der Konfigurationsmenüs

Abbildung 4-2 zeigt, wie die Menüs und Profile in der Pipeline-Software organisiert sind.

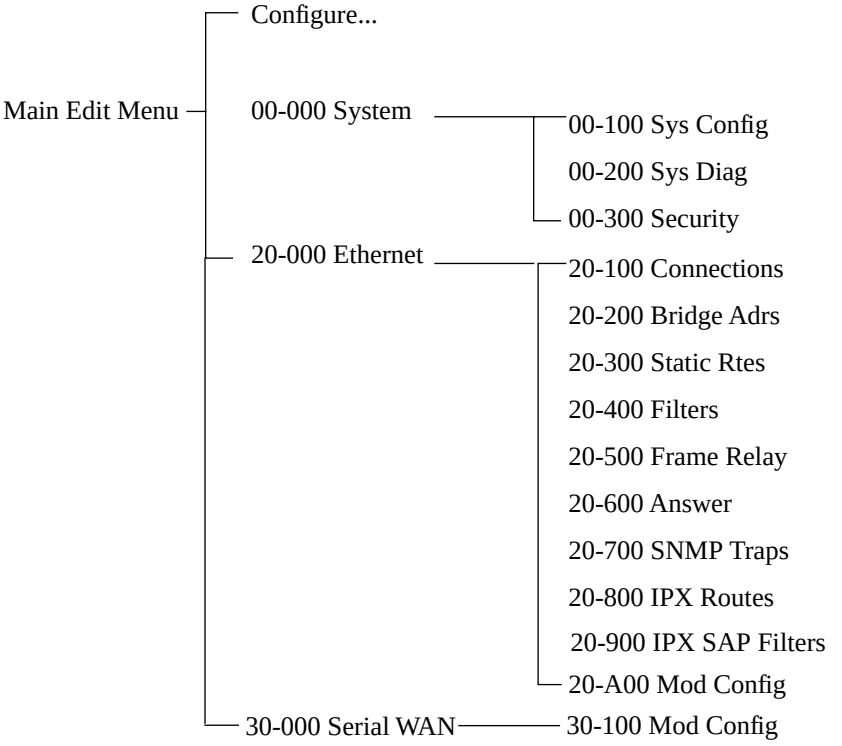


Abbildung 4-2: Organisation der Menüs und Profile in der Pipeline-Software

Aktivieren von Menü- bzw. Statusfenstern

Es kann immer nur ein Fenster (Menü- oder Statusfenster) aktiv sein. Das aktive Fenster ist durch eine dicke Doppellinie links, rechts und oben gekennzeichnet.

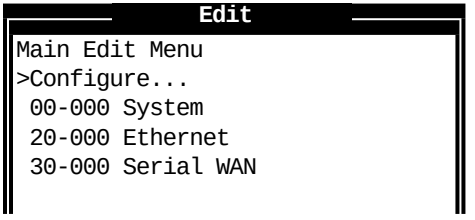
In Abbildung 4-1 ist das Statusfenster „10-100“ das aktive Fenster (oben in der Mitte).

Wenn Sie die Tabulatortaste drücken, wird das Fenster „00-200“, also das nächste Fenster rechts, zum aktiven Fenster. Durch weiteres Drücken der Tabulatortaste wechselt das aktive Fenster immer weiter von links nach rechts und von oben nach unten, bis Sie das letzte Fenster in der rechten unteren Ecke erreicht haben. Wenn Sie ein Fenster links vom gerade aktiven Fenster aktivieren wollen, können Sie mit der Tastenkombination Rücktaste-Tab bzw. Strg-O die Richtung umkehren.

Öffnen der Menüs und Profile

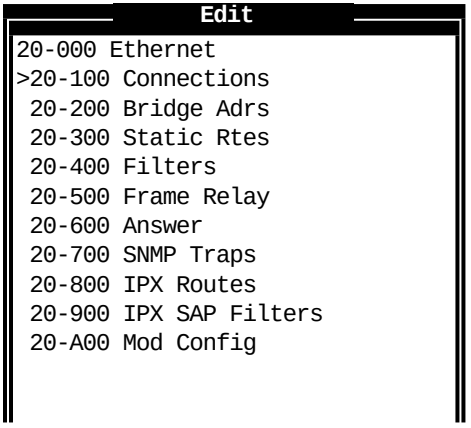
Das „Main Edit Menu“ enthält eine Liste mit Menüs, die jeweils Profile und Untermenüs enthalten können.

Im jeweils aktiven Menü zeigt das Cursor-Zeichen (>) auf eines der Menüelemente. Um den Cursor eine Zeile nach unten zu verschieben, ist Strg-N („Next“) bzw. die Nach-unten-Pfeiltaste zu drücken. Mit Strg-P („Previous“) bzw. der Nach-oben-Pfeiltaste können Sie den Cursor nach oben verschieben. (Die Pfeiltasten werden von einigen VT100-Emulatoren nicht unterstützt.)

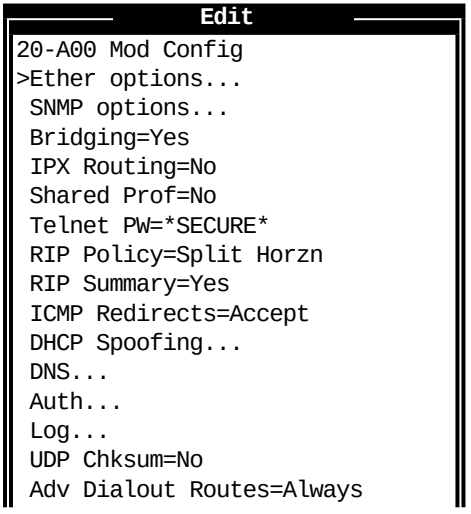


Ein Menü öffnen Sie, indem Sie mit dem Cursor den jeweiligen Menünamen markieren und dann die Eingabetaste drücken. Um z. B. das Menü „20-000 Ethernet“ zu öffnen, müssen Sie die Tastenkombination Strg-N so lange drücken,

bis der Cursor auf diesen Menünamen zeigt. Wenn Sie nun die Eingabetaste drücken, wird das Menü „Ethernet“ geöffnet.



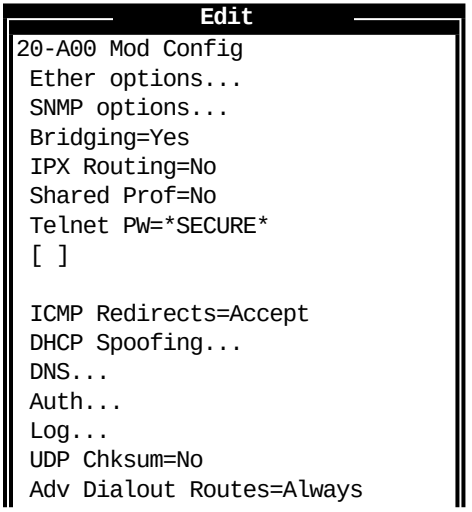
Das Menü „Ethernet“ enthält Untermenüs und Profile, die mit Netzwerkfunktionen wie Bridging, Routing, WAN-Verbindungen usw. zu tun haben. Über den Menüpunkt „Mod Config“ können Sie ein Untermenü öffnen, das Optionen zur Konfiguration der Ethernet-Schnittstelle selbst enthält:



Hinweis: Mit Ausnahme der mit „N/A“ („not applicable“ = nicht zutreffend) gekennzeichneten Parameter können sämtliche Parameter in allen Profilen geändert werden. Unter dem Begriff „Profil“ wird eine Gruppe von Parametern verstanden, die unter einem bestimmten Menüeintrag aufgeführt werden. Nicht zutreffende Parameter (N/A) sind Parameter, für die es aufgrund der Einstellung anderer Parameter oder Profile keinen sinnvollen bzw. gültigen Wert gibt.

Öffnen der Bearbeitungsfelder

Um das Bearbeitungsfeld für einen auf Texteingabe beruhenden Parameter (wie z B. ein Kennwort) zu öffnen, muß der jeweilige Parameter mit dem Cursor markiert und anschließend die Eingabetaste gedrückt werden. Es öffnet sich ein durch eckige Klammern begrenztes Bearbeitungsfeld. Siehe dazu das folgende Beispiel für den Parameter „Telnet PW“:



Hinweis: Weitere Informationen zu diesem Parameter finden Sie im Abschnitt „Pipeline-Kennwörter“ auf Seite 4-9.

Zwischen den Klammern erscheint ein blinkender Text-Cursor und zeigt so an, daß Sie mit der Eingabe von Text beginnen können. Befindet sich im Feld bereits Text, wird dieser gelöscht, sobald Sie ein Zeichen eingeben. Sollen nur einige Zeichen des bereits zwischen den Klammern angezeigten Textes geändert werden, können Sie mit Hilfe der Pfeiltasten den Text-Cursor an der entsprechenden Stelle positionieren und dann das Zeichen löschen oder überschreiben.

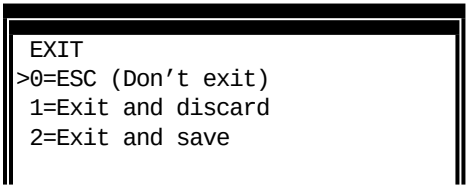
Um das Bearbeitungsfeld zu schließen und den neuen Text wirksam werden zu lassen, müssen Sie die Eingabetaste drücken.

Festlegen der Werte für Zahlenparameter

Ein Zahlenparameter ist ein Parameter, für den es mehrere vordefinierte Werte gibt. Sie können Zahlenparameter ändern, indem Sie den Parameter mit dem Cursor markieren und so lange die Eingabetaste bzw. die Nach-rechts-Taste drücken, bis der gewünschte Wert erscheint.

Speichern der Änderungen

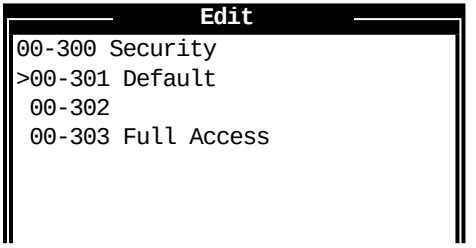
Wenn Sie ein Profil verlassen, werden Sie gefragt, ob die Änderungen gespeichert werden sollen.



Wenn Sie die aktuellen Profilwerte speichern wollen, markieren Sie die Option „Exit and Save“, und drücken Sie die Eingabetaste oder die Taste 2.

Pipeline-Kennwörter

Die Pipeline verfügt über drei Sicherheitsstufen, die jeweils in einem eigenen „Security“-Profil gespeichert sind. Bei Auslieferung der Pipeline ab Werk sind alle Sicherheitsstufen total offen, d. h., es sind keinerlei Zugriffseinschränkungen definiert. Um sich die Liste der „Security“-Profile anzusehen, müssen Sie das Menü „System“ im „Main Edit Menu“ öffnen, die Option „Security“ markieren und dann die Eingabetaste drücken.



Sobald die Pipeline eingeschaltet wird, aktiviert sie das erste „Security“-Profil in dieser Liste. Dieses trägt stets den Namen „Default“, und ihm ist immer kein Kennwort zugewiesen. Die meisten Administratoren ändern als erstes die Zugriffsrechte im „Default“-Profil, um die Funktionen einzuschränken, die von allen genutzt werden können, die auf die Pipeline-Konfigurationsmenüs zugreifen können. Dazu sind vier Schritte erforderlich, deren Befolgung dringend zu empfehlen ist:

1 Öffnen Sie das „Security“-Profil „Default“, und legen Sie für den Parameter „Operations“ den Wert „No“ fest.

2 Weisen Sie dem „Security“-Profil „Full Access“ ein Kennwort zu. (Schränken Sie jedoch nicht die Zugriffsrechte im „Full-Access“-Profil ein.)

3 Aktivieren Sie das „Security“-Profil „Full Access“, und fahren Sie mit der Konfiguration der Pipeline fort.

Eine ausführliche Beschreibung der „Security“-Profile und der Zuweisung von Kennwörtern finden Sie im Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Achtung: Wenn Sie nun die Pipeline zurücksetzen oder einschalten, wird das neue, eingeschränkte „Default“-Profil aktiviert. Konfigurationsaufgaben können erst dann ausgeführt werden, wenn Sie das Kennwort für das „Full-Access“-Profil aktiviert und eingegeben haben. Das Standard-Kennwort für das „Full-Access“-Profil lautet „Ascend“.

Zur Aktivierung des „Security“-Profils „Full-Access“ ist die Tastenkombination Strg-D zu drücken. Daraufhin wird ein kontextsensitives Menü, das sogenannte „DO-Menü“ angezeigt.

```
Edit
00-300 Security
DO...
>0=ESC
 P=Password
```

Drücken Sie im DO-Menü die Taste P (oder wählen Sie „P=Password“). Es erscheint die Liste der „Security“-Profile. Markieren Sie „Full Access“, und drücken Sie die Eingabetaste. Die Pipeline fordert zur Eingabe des Kennworts für dieses Profil auf.

```
Edit
00-300 Security
Enter Password:
 []

 Press > to accept
```

Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste. (Es wird empfohlen, das Standard-Kennwort „Ascend“ des „Full-Access“-Profils so schnell wie möglich durch ein anderes Kennwort zu ersetzen.)

Wenn Sie das richtige Kennwort eingegeben haben, erscheint eine Meldung, die besagt, daß das Kennwort akzeptiert wurde und daß die Pipeline jetzt die neue Sicherheitsstufe verwendet. Wurde das Kennwort falsch eingegeben, werden Sie aufgefordert, es noch einmal zu versuchen.

Hinweis: Bei Konsolensitzungen, die über Telnet aufgebaut werden, kann die Telnet-Sitzung erst dann zustandekommen, wenn die rufende Seite das Telnet-Kennwort angegeben hat. (Als Standard muß einfach nur die Eingabetaste gedrückt werden.) Für diese Sitzung gelten dann die Einstellungen im „Security“-Profil „Default“. Wenn die Pipeline über Telnet konfiguriert werden soll, muß die rufende Seite das entsprechende „Security“-Profil aktivieren.

Sonderzeichen und Tastenkombinationen für die Menü- und Statusfenster

Die folgenden Zeichen haben in den Menü- und Statusfenstern eine besondere Bedeutung:

- Das Pluszeichen (+) zeigt an, daß der von Ihnen eingegebene Text zu lang ist, um auf eine Zeile zu passen. Er wird daher in der Fensteranzeige abgeschnitten.
- Drei Punkte (…) zeigen an, daß es für das jeweilige Menüelement ein Untermenü mit weiteren Optionen gibt.

  Das Untermenü wird angezeigt, wenn Sie das entsprechende Menüelement markieren.

In der folgenden Tabelle finden Sie alle Spezialtasten bzw. Tastenkombinationen für die Arbeit in den Menü- und Statusfenstern des „Control Monitors“.

Tabelle 4-1: „Control-Monitor“-Spezialtasten und -Tastenkombinationen

Taste/Tastenkombination	Operation
Nach-rechts-Pfeiltaste, Eingabetaste, Strg-Z, Strg-F	Zahlenparameter: nächsten Wert auswählen Textparameter: ein Zeichen nach rechts gehen bzw. gegenwärtigen Wert akzeptieren Menü: aktuelle Auswahl öffnen
Nach-links-Pfeiltaste, Strg-X, Strg-B	Zahlenparameter: vorherigen Wert auswählen Textparameter: ein Zeichen nach rechts gehen bzw. gegenwärtige Eingabe verlassen Menü: aktuelle Auswahl schließen
Nach-unten-Pfeiltaste, Strg-N	Cursor eine Zeile nach unten bewegen
Nach-oben-Pfeiltaste, Strg-U, Strg-P	Cursor eine Zeile nach oben bewegen
Strg-V	zur nächsten Seite in der Liste springen
Tab, Strg-I	zum nächsten Fenster springen
Rücktaste-Tab, Strg-O	zum vorherigen Fenster zurückkehren
Entf	Zeichen unter dem Cursor löschen
Rücktaste	Zeichen links vom Cursor löschen
Strg-D	DO-Menü öffnen
Strg-L	VT-100-Bildschirm aktualisieren
D	aktuelles Profil wählen

Hinweis: Die Strg- und die Umschalttaste werden stets in Kombination mit anderen Tasten verwendet. Solche Tastenkombinationen werden in diesem Dokument mit einem Bindestrich zwischen den jeweiligen Tastenbezeichnungen dargestellt, wie z. B. bei der Tastenkombination Umschalt-T, mit der Sie ein großes T eingeben können.

Wie geht's weiter?

Nachdem Sie nun die Arbeit mit der Pipeline-Benutzeroberfläche gelernt haben, können Sie entweder die Anweisungen im nächsten Kapitel befolgen, um die Konfiguration Ihrer Pipeline abzuschließen, oder aber anhand der folgenden Liste eine Entscheidung treffen, was als nächstes geschehen soll.

- Im Kapitel 5, „Konfigurieren von WAN-Verbindungen", finden Sie Informationen zur Konfiguration der WAN-Schnittstellen.
- Im Kapitel 6, „Konfigurieren der Pipeline als Bridge", finden Sie Informationen zur Konfiguration der Pipeline für das Bridging.
- Im Kapitel 7, „Konfigurieren der Pipeline als IP-Router", finden Sie Informationen zur Konfiguration der Pipeline für das IP-Routing.
- Im Kapitel 8, „Konfigurieren der Pipeline als IPX-Router", finden Sie Informationen zur Konfiguration der Pipeline für das IPX-Routing.

Konfigurieren von WAN-Verbindungen

5

Dieses Kapitel enthält die folgenden Abschnitte:

Hinweis: In diesem Kapitel wird nicht erklärt, wie Netzwerkverbindungen für das IP-Routing, das IPX-Routing oder das Bridging auf Verbindungsebene zu konfigurieren sind. Zu diesen Themenbereichen gibt es jeweils eigene Kapitel weiter hinten in diesem Handbuch.

Einführung

In diesem Abschnitt werden die Grundelemente des Aufbaus von WAN-Verbindungen mit Hilfe einer Pipeline beschrieben. Folgende Themen werden behandelt:

- Einkapselungsverfahren
- Gruppen
- Festverbindungen
- Initiierung von Rufen durch die Pipeline
- Beantwortung von Rufen durch die Pipeline
- das Antwortprofil
- das Verbindungsprofil

Einkapselungsverfahren

Neben den grundlegenden telefongesellschaftsspezifischen Optionen und Authentifizierungsverfahren müssen die rufende und die antwortende Seite einer Verbindung vor allem auch aushandeln, welches Verfahren zur Verbindungseinkapselung verwendet werden soll. Die rufende Seite muß alle abgehenden Pakete „verpacken“ (einkapseln), bevor diese über das WAN gesendet werden können. Das antwortende Gerät hat dann diese Pakete wieder „auszupacken“, bevor es die Pakete weiterleitet. Die Pipeline unterstützt die folgenden Einkapselungsverfahren:

- PPP und MP+

  Das Hauptanwendungsgebiet für PPP (Point-to-Point Protocol)- und MP+ (Multilink Protocol Plus)-Verbindungen ist die Herstellung von Verbindungen zu anderen PPP-Bridges, -Routern und -Hosts.

  Mit PPP werden Einkanalverbindungen mit anderen Geräten hergestellt, auf denen ebenfalls PPP eingesetzt wird. MP und MP+ sind Erweiterungen von PPP zur Unterstützung von Mehrkanalverbindungen. Wenn eine Verbindung für MPP eingerichtet ist, versucht die Pipeline zunächst, eine MP+-Verbindung herzustellen. Wird MP+ von der anderen Seite der Verbindung nicht unterstützt, fordert die Pipeline MP an. Wenn dieses Protokoll ebenfalls abgelehnt wird, kommt statt dessen PPP zum Einsatz. Daher wird der Begriff „PPP-Verbindung“ auch häufig zur Bezeichnung einer dieser

Einkapselungsverfahren verwendet, wenn die Anzahl der Kanäle keine Rolle spielt.

PPP-Verbindungen unterstützen die PAP- und CHAP-Kennwort-Authentifizierung. Außerdem wird IP-Routing, IPX-Routing und protokollunabhängiges Bridging unterstützt. Bei PPP-Verbindungen kann es sich sowohl um gewählte ankommende als auch um gewählte abgehende Verbindungen handeln.

- Frame Relay RFC 1490

  Frame-Relay-Verbindungen werden hauptsächlich zur Verbindung mit Frame-Relay-Vermittlungsstellen eingesetzt. Es wird keine Authentifizierung unterstützt.

  Frame-Relay-Gateway-Verbindungen unterstützen Routing und Bridging zwischen der Pipeline und der Vermittlungsstelle über eine Festverbindung (Mietleitung).

  Einige Ascend-Einheiten bieten Frame-Relay-Operationen als Software-Option.

Gruppen von Festverbindungen

Eine Festverbindung ist eine permanente Verbindung, die stets verbunden ist, solange eine physikalische Verbindung besteht. Bei einer Zurücksetzung der Einheit oder der zentralen Vermittlungsstellen bzw. bei einer Unterbrechung der Verbindung versucht die Pipeline in Abständen von jeweils 10 Sekunden, die Verbindung wiederherzustellen. Wird die Pipeline oder das Gerät auf der anderen Seite der Verbindung ausgeschaltet, wird die Verbindung wiederhergestellt, sobald beide Geräte wieder mit Strom versorgt werden.

Bei ISDN-Leitungen verwendet die Festverbindung einen der Kanäle der Leitung. Verbindungen über die serielle WAN-Schnittstelle und Frame-Relay-Verbindungen sind nicht kanalisiert und stets 100 % festgeschaltet.

Damit die Kanäle von Festverbindungen genutzt werden können, müssen die Kanäle für diese Nutzung eingerichtet sein und einer Gruppennummer zugewiesen werden.

Hinweis: Bei der Vergabe der Gruppennummern ist darauf zu achten, daß diese für alle WAN-Schnittstellen eindeutig sein müssen.

Für die WAN-Schnittstellen der Pipeline werden die folgenden Gruppennummern empfohlen:

- Wird für den Parameter „Chan Usage“ der Wert „Leased/Switch“ festgelegt, lautet die Gruppennummer für den ersten B-Kanal 1 (kann nicht geändert werden).
- Wird für den Parameter „Chan Usage“ der Wert „Switch/Leased“ festgelegt, lautet die Gruppennummer für den zweiten B-Kanal 2 (kann nicht geändert werden).
- Bei seriellen WAN-Schnittstellen ist für die Gruppennummer der Wert 3 festzulegen.

In welchem Profil die Zuweisung von Kanälen zu den einzelnen Gruppen erfolgt, hängt von der Art der Leitung ab, mit der die Verbindung hergestellt wird:

- Bei Verbindungen zu anderen Routern/Bridges, bei denen die PPP-Einkapselung zur Anwendung kommt, wird die Gruppennummer mit Hilfe des Parameters „Group“ im Untermenü „Telco options“ des Verbindungsprofils festgelegt.
- Bei Verbindungen mit Frame-Relay-Einkapselung wird die Gruppennummer mit Hilfe des Parameters „Nailed Grp“ im Frame-Relay-Profil festgelegt.
- Bei Verbindungen über die serielle WAN-Schnittstelle wird die Gruppennummer mit Hilfe des Untermenüs „Mod Config“ im „Serial-WAN“-Profil festgelegt.

Initiierung von Rufen durch die Pipeline

Die Pipeline initiiert eine Bridging-Verbindung über das WAN, sobald sie Pakete empfängt, deren Ziele sich nicht im lokalen LAN befinden, bzw. sobald sie ein Broadcast-Paket empfängt. Die Pipeline initiiert geroutete Verbindungen nur dann, wenn es eine Route zum Ziel gibt. Außerdem versucht die Pipeline nicht, jedes Paket zu routen. Sie routet nur dann alle Pakete, wenn sie als Standard-Gateway konfiguriert wurde.

Soll eine Verbindung manuell gewählt werden, müssen Sie die Tastenkombination Strg-D drücken, um das DO-Menü aufzurufen, und dann den Befehl „DO Dial“ wählen. Näheres zum manuellen Initiieren von Rufen finden Sie im Kapitel 11, „Systemadministration“.

Informationen dazu, wie die Pipeline Bridging- und Routing-Verbindungen aufbaut, können Sie Kapitel 6, „Konfigurieren der Pipeline als Bridge“, Kapitel 7, „Konfigurieren der Pipeline als IP-Router“ und Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“ entnehmen.

Zur Steuerung der Herstellung von WAN-Sitzungen durch die Pipeline stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Die Verwendung von Filtern, um zu verhindern, daß bestimmte Pakete, wie Broadcasts oder IPX-RIP- bzw. -SAP-Abfragen, eine Verbindung zum entfernten Netzwerk herstellen. Informationen zum Erstellen von Filtern finden Sie im Kapitel 10, „Definieren von Filtern“.
- Wird die Pipeline als Bridge eingesetzt, kann sie (mit Hilfe des Parameters „Dial Brdcast“) so konfiguriert werden, daß sie keine Rufe initiiert, wenn sie Broadcasts empfängt. Informationen zum Konfigurieren von Bridging-Verbindungen entnehmen Sie bitte Kapitel 6, „Konfigurieren der Pipeline als Bridge“.
- Wird die Pipeline zum IPX-Routing eingesetzt, kann sie (mit Hilfe des Parameters „Dial Query“) so konfiguriert werden, daß sie keine Rufe initiiert, wenn sie IPX-Anfragen empfängt. Informationen zum Konfigurieren von IPX-Routing-Verbindungen entnehmen Sie bitte Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“.

Beantwortung von Rufen durch die Pipeline

Bevor die Pipeline ankommende Rufe beantwortet, überprüft sie das Antwortprofil daraufhin, ob eine CLID-Authentifizierung stattfinden soll. Wenn die CLID-Authentifizierung gefordert wird und die Telefonnummer nicht mit einem Verbindungsprofil übereinstimmt, bricht die Pipeline den Ruf ab. Ist keine CLID-Authentifizierung erforderlich oder wurde ein entsprechendes Verbindungsprofil gefunden, beantwortet die Pipeline den Ruf und führt die folgenden Schritte aus:

- Wird das von der rufenden Seite verwendete Einkapselungsverfahren unterstützt?

  Die Pipeline unterstützt die Einkapselungsverfahren PPP, MPP, MP und Frame Relay. Verwendet ein Ruf keines dieser Verfahren, bricht die Pipeline den Ruf ab.

  Hinweis: Bei MP+-Verbindungen willigt die Pipeline zunächst ein, PPP zu verwenden. Wird vom rufenden Ende MP+ angefordert, überprüft die Pipeline im Antwortprofil, ob MPP aktiviert ist. Ist dies nicht der Fall, wird statt dessen das standardmäßige PPP verwendet.

- Ist eine Authentifizierung erforderlich?

  Bei PPP- bzw.- MP+-Rufen kann das Antwortprofil PAP- oder CHAP-Authentifizierung verlangen (Parameter „Recv Auth“).

  Frame Relay unterstützt Wählleitungen (gewählte Leitungen) nicht, so daß auch keine Ruf-Authentifizierung stattfindet.

  Wenn Authentifizierung erforderlich ist, muß ein passendes Verbindungsprofil gefunden werden. Erfordert das Antwortprofil nicht das Vorhandensein eines Verbindungsprofils (wenn „Profile Reqd=No“ festgelegt wurde und keine Authentifizierung erforderlich ist), kann die Verbindung u. U. mit Antwortprofil-Parametern aufgebaut werden.

- Gibt es ein passendes Verbindungsprofil?

  Die Pipeline kann nur Verbindungsprofile verwenden, die ankommende Rufe unterstützten, um solche Rufe anzunehmen. Dies wird im Parameter „AnsOrig“ festgelegt.

  Die Pipeline sucht nach einem Verbindungsprofil, das den Namen der rufenden Seite und das entsprechende Kennwort enthält. Wird keine Kennwort-Authentifizierung benötigt, kann die Pipeline PPP-Rufe für das

IP-Routing mit den in den Verbindungsprofilen (im Parameter „LAN Adrs“) eingetragenen IP-Adressen vergleichen.

- Herstellen der Verbindung

  Nach erfolgreicher Authentifizierung baut die Pipeline die Verbindung entsprechend den Verbindungsprofil-Einstellungen für das Einkapselungsverfahren, die „Telco options“ und die Sitzung auf. Wenn die Pipeline so konfiguriert wurde, daß keine Authentifizierung oder kein Verbindungsprofil erforderlich ist, verwendet sie für den Aufbau der Verbindung das Antwortprofil.

- Weiterleiten der Pakete

  Die Pipeline leitet dann den Ruf an die Bridging-/Routing-Software weiter und beginnt mit dem Routing der Pakete.

Hinweis: Wurde im Ethernet-Profil ein Telnet-Kennwort („Telnet PW“) festgelegt, wird der Benutzer bei Telnet-Verbindungen mit der Pipeline, unabhängig von der Art des Rufes und der Authentifizierung, aufgefordert, das Telnet-Kennwort einzugeben. Dieses Kennwort muß auch von Telnet-Benutzern eingegeben werden, die über die Ethernet-Schnittstelle verbunden sind.

Optionen für die Datenkomprimierung

Damit eine Datenkomprimierung stattfinden kann, müssen beide Seiten der Verbindung dasselbe Verfahren unterstützen. Die Pipeline unterstützt die folgenden Datenkomprimierungsverfahren:

- „Stac“ für Rufe mit PPP-Einkapselung

  Bei der Stac-Komprimierung wird ein von der Firma STAC Electronics, Inc. entwickelter Komprimierungsalgorithmus verwendet, der den Standard-LZS-Komprimierungsalgorithmus so modifiziert, daß die Komprimierungsgeschwindigkeit optimiert wird (zu Lasten des Komprimierungsgrads). Wenn Sie für das Gerät STAC-Komprimierung festlegen und das Gerät am anderen Ende ebenfalls STAC-Komprimierung unterstützt, wird diese beim Aushandeln einer PPP-Verbindung eingerichtet.

- „MS-Stac“ für Rufe mit PPP-Einkapselung

  MS-Stac steht für die Microsoft LZS Coherency Compression für Windows 95 und ist ein nur unter Windows 95 (nicht unter Windows NT) einsetzbares proprietäres Komprimierungsverfahren.

Hinweis: Wenn von der rufenden Seite „MS-Stac“ angefordert wird, dies aber nicht im Verbindungsprofil festgelegt wurde, scheint die Verbindung zwar ordnungsgemäß aufgebaut zu werden, es werden aber keine Daten „geroutet“. Ist im Verbindungsprofil „MS-Stac“ festgelegt und wird dieses Komprimierungverfahren von der rufenden Seite nicht bestätigt, versucht die Pipeline, den Standardwert „Stac“ zu verwenden. Ist dies nicht möglich, erfolgt keinerlei Komprimierung.

- „VJ Comp“ für TCP/IP-Verbindungen
  „VJ Comp“ wird nur bei Paketen in TCP-Anwendungen, wie z. B. Telnet, verwendet. Wenn Sie dieses Komprimierungsverfahren einschalten, werden auf beiden Seiten der Verbindung die TCP/IP-Header komprimiert.

Das Antwortprofil

Bevor die Pipeline einen ankommenden Ruf beantwortet, sucht sie in ihrem Antwortprofil nach Informationen darüber, wie weiter vorzugehen ist. Enthält der Ruf nicht die für das Antwortprofil erforderlichen Informationen (wie Name und Kennwort), hängt die Pipeline auf.

Wenn der Ruf allerdings die erforderlichen Informationen enthält, sucht die Pipeline nach einem Verbindungsprofil. Findet sie eines, zieht sie dessen Parametereinstellungen denen des Antwortprofils vor.

Hinweis: Wenn für „Profile Reqd“ der Wert „No“ festgelegt wurde, kann der Ruf u. U. mit Hilfe spezifischer Einstellungen im Antwortprofil aufgebaut werden.

Das Antwortprofil enthält die in der Tabelle 5-1 aufgeführten Parameter.

Tabelle 5-1: Parameter im Antwortprofil

Ort	Parameter
Ethernet > Answer (Antwortprofil)	Force 56=No Profile Reqd=Yes ID Auth=Ignore
Ethernet > Answer > PPP options...	Route IP=Yes Route IPX=Yes Bridge=Yes Recv Auth=Either MRU=1524 LQM=No LQM Min=600 LQM Max=600 Link Comp=Stac VJ Comp=Yes Dyn Alg=Quadratic Sec History=15 Add Pers=5 Sub Pers=10 Min Ch Count=1 Max Ch Count=1 Target Util=70 Idle Pct=0

Genauere Angaben zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Zum Einrichten eines grundlegenden Antwortprofils ist wie folgt vorzugehen:

1 Öffnen Sie das Antwortprofil.

2 Legen Sie fest, daß für ankommende Rufe ein entsprechendes Profil vorhanden sein muß.

```
Profile Reqd=Yes
```

Mit dieser Einstellung wird die Pipeline gehindert, Verbindungen auf der Grundlage der Parameter im Antwortprofil aufzubauen.

3 Schalten Sie, falls gewünscht, die CLID-Authentifizierung ein.

Beispiel:

```
ID Auth=Accept
```

Einige Verbindungsarten verfügen über keine eigenen Authentifizierungsverfahren. Wenn Sie solche Rufarten zulassen wollen, empfiehlt es sich u. U., die CLID-Authentifizierung zu verwenden. Siehe dazu Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Zum Festlegen der Optionen für PPP- und MP+-Rufe ist wie folgt vorzugehen:

4 Öffnen Sie das Untermenü „PPP Options“.

5 Geben Sie an, ob die Verbindung Routing oder/und Bridging unterstützen soll.

Beispiel:

```
Route IP=Yes
Route IPX=Yes
Bridge=Yes
```

Hinweis: Für das Routing bzw. Bridging in einem Verbindungsprofil muß Routing bzw. Bridging unter „Mod Config“ bzw. im „Configure“-Profil global aktiviert sein.

6 Geben Sie an, ob die PAP- oder/und CHAP-Authentifizierung verwendet werden soll.

Beispiel:

```
Recv Auth=Either
```

Wird für diesen Parameter der Wert „None“ festgelegt, müssen ankommende MP+- oder PPP-Rufe kein Kennwort angeben. Ist für „Recv Auth“ nicht „None“ eingestellt, müssen ankommende Rufe ein Verbindungsprofil haben.

Näheres zu PAP und CHAP erfahren Sie im Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

7 Nehmen Sie die gewünschten Einstellungen für die Bandbreitenparameter vor.

Die Bandbreitenparameter im Antwortprofil gelten für ankommende Rufe, für die kein Verbindungsprofil existiert. Dort, wo es ein Verbindungsprofil gibt, gelten dessen Parameterwerte.

Siehe dazu „Dynamische Bandbreitenzuweisung (DBA)“ auf Seite 5-18.

8 Schließen Sie das Antwortpr ofil.

Verbindungsprofile

Ein Verbindungsprofil enthält Parameter für die Einrichtung einer einzelnen Verbindung.

In Verbindungsprofilen sind die in der Tabelle 5-2 aufgeführten Parameter zu finden.

Tabelle 5-2: Parameter in Verbindungsprofilen

Ort	**Parameter**
Ethernet > Connection > alle Profile (Verbindungsprofil)	Station=[] Active=No Encaps=*Einkapselungsverfahren* Dial #=[] Calling #=[] Route IP=No Route IPX=No Bridge=Yes Dial brdcast=No
Ethernet > Connection > alle Profile > Encaps options...	*Abhängig vom jeweiligen Einkapselungsverfahren* Siehe: • „Konfigurieren einer PPP-Verbindung“ auf Seite 5-14 • „Konfigurieren einer MP- oder MP+-Verbindung“ auf Seite 5-16 • „Konfigurieren von Frame-Relay-Verbindungen“ auf Seite 5-26

Tabelle 5-2: Parameter in Verbindungsprofilen

Ort	Parameter
Ethernet > Connection > alle Profile > IP options...	Siehe Kapitel 7, „Konfigurieren der Pipeline als IP-Router“
Ethernet > Connection > alle Profile > IPX options...	Siehe Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“
Ethernet > Connection > alle Profile > Session options...	Data Filter=0 Call Filter=0 Idle=120 Preempt=60 IPX SAP Filter=0 BackUp=N/A Secondary=
Ethernet > Connection > alle Profile > Telco options...	AnsOrig=Ans Only Callback=No Call Type=Switched Group=N/A FT1 Caller=N/A Data Svc=56KR Force 56=N/A Bill #=[]

Genauere Angaben zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Überblick über die Sitzungsoptionen

Jedes Verbindungsprofil enthält eine Gruppe von Sitzungsparametern für die Verwaltung von WAN-Sitzungen. So können Sie zum Beispiel einen Filter zuweisen, um zu verhindern, daß Verbindungen durch routinemäßigen Netzwerkverkehr dauerhaft aktiv bleiben (siehe Kapitel 10, „Definieren von Filtern“).

Der Parameter „Idle“ gibt an, wie viele Sekunden der Inaktivität die Pipeline abwartet, bis sie den Ruf unterbricht. Wird für diesen Parameter der Wert „0“ (Null) festgelegt, können Sitzungen uneingeschränkt inaktiv bleiben.

Der Parameter „Preempt“ gibt an, wie viele Sekunden der Inaktivität die Pipeline wartet, bis sie einen der Kanäle der inaktiven Verbindung für einen neuen Ruf verwendet. Es kann eine Zahl zwischen 0 und 65535 angegeben werden. Wird für diesen Parameter der Wert „0“ (Null) festgelegt, können Sitzungen uneingeschränkt inaktiv bleiben, ohne daß einer der Kanäle anderweitig genutzt wird. Die Standardeinstellung ist „60“.

Überblick über die telefongesellschaftsspezifischen Optionen („Telco options“)

Jedes Verbindungsprofil enthält eine Gruppe von telefongesellschaftsspezifischen Optionen („Telco options“):

- „AnsOrig“
  Sie können festlegen, ob die Pipeline diese Verbindung initiieren, einen ankommenden Ruf beantworten oder beides soll. Der Standardwert ist „Both“.
- „Callback“ (Leistungsmerkmal „Rückruf“)
  Mit Hilfe des Parameters „Callback“ können Sie die Pipeline anweisen, bei ankommenden gewählten Rufen sofort nach Empfang des Rufes aufzulegen und das Gerät am entfernten Ende der Verbindung unter Nutzung der im Verbindungsprofil angegebenen Rufnummer (Parameter „Dial #“) zurückzurufen.
- „Data Svc“ und „Force 56“
  Der ausgewählte Datendienst muß von Ende zu Ende verfügbar sein.
- „Call Type“, „Group“ und „FT1 Caller“
  Der Parameter „Call Type“ ist standardmäßig auf „Switched“ eingestellt. Die anderen Optionen sind „Nailed“, „Nailed/MPP“ und „Perm/Switched“.

Eine Festverbindung ist eine permanente Verbindung, die so lange aufrechterhalten bleibt, wie eine physikalische Verbindung besteht. Bei Festverbindungen muß die Gruppennummer der festgeschalteten Kanäle angegeben werden.

Beispiel:

```
Call Type=Nailed
Group=3
```

In einer Verbindung, bei der der Parameter „Call Type“ auf „Nailed/MPP“ gesetzt wurde, bestehen festgeschaltete und gewählte Kanäle nebeneinander. Wenn Sie diesen Ruftyp wählen, muß angegeben werden, welche Seite der Verbindung gewählte Kanäle hinzufügen kann (Parameter „FT1 Caller“). Ausführliche Informationen zum Ruftyp „Nailed/MPP“ finden Sie im Abschnitt „MPP-Festverbindungen“ auf Seite 5-24.

Hinweis: Permanente Wählverbindungen (gewählte Verbindungen) sind abgehende gewählte Rufe, die versuchen, ständig aufrechterhalten zu bleiben. Wird die Einheit oder der zentrale Switch zurückgesetzt oder die physikalische Verbindung unterbrochen, versucht die permanente Wählverbindung alle 10 Sekunden, die physikalische Verbindung wiederherzustellen. Dies ähnelt der Art und Weise, wie Festverbindungen aufrechterhalten werden. Mit permanenten Wählverbindungen kann die Anzahl der Wählversuche reduziert werden, wobei jedoch sehr lange Verbindungszeiten entstehen können. Abhängig von der jeweiligen Abrechnungsmethode kann dies für einige Kunden Kostenvorteile mit sich bringen. Näheres dazu können Sie dem *Referenzhandbuch* entnehmen.

Konfigurieren einer PPP-Verbindung

PPP-Verbindungen verwenden für Einkanalrufe das PPP-Einkapselungsverfahren. Zur Konfiguration einer PPP-Verbindung sind die folgenden Hauptschritte auszuführen:

- Bestimmen der entsprechenden Routing-, Authentifizierungs- und Komprimierungseinstellungen
- Überprüfen, ob die PPP-Optionen im Antwortprofil konfiguriert sind
- Konfigurieren der PPP-Verbindung in einem Verbindungsprofil
- Konfigurieren der Routing- bzw. Bridging-Einstellungen in der Pipeline und für die WAN-Verbindung

Hinweis: In diesem Abschnitt wird davon ausgegangen, daß das Antwortprofil so eingerichtet wurde, daß PPP-Verbindungen zugelassen sind (siehe dazu „Das Antwortprofil“ auf Seite 5-8). Einzelheiten zur Konfiguration der Routing- und

Bridging-Einstellungen entnehmen Sie bitte den entsprechenden Kapiteln weiter hinten in diesem Handbuch.

PPP-Verbindungen sind im Normalfall „gebridgte“ oder „geroutete“ Netzwerkverbindungen, die mit Hilfe einer PPP-Wählsoftware initiiert wurden.

Für PPP-Konfigurationen stehen die folgenden Parameter zur Verfügung:

Tabelle 5-3: Parameter für PPP-Verbindungen

Ort	**Parameter**
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Encaps=PPP
Ethernet > Connections > *alle Profile* > Encaps options...	Send Auth=CHAP Send PW=*SECURE* Recv PW=*SECURE* MRU=1524 LQM=No LQM Min=600 LQM Max=600 Link Comp=Stac VJ Comp=Yes

Namen für die Pipeline festlegen:

1 Öffnen Sie das Systemprofil.

2 Geben Sie im Parameter „Name“ einen Namen für die Pipeline-Einheit an.
Beispiel:
`Name=MEINEPIPE1`
Für diesen Parameter muß ein Wert festgelegt werden, wenn „Send Auth= PAP“ oder „Send Auth=CHAP“ festgelegt wurde.

3 Schließen Sie das Systemprofil.

Konfigurieren einer PPP-Verbindung:

1 Öffnen Sie das Verbindungsprofil.

2 Geben Sie im Parameter „Station“ den Namen des entfernten Geräts an.

Beispiel:

```
Station=andereseite
```

Beachten Sie, daß der Name genau wie angegeben eingegeben werden muß, einschließlich aller Groß- bzw. Kleinbuchstaben, Leerzeichen bzw. Unterstriche.

3 Aktivieren Sie das Profil.

```
Active=Yes
```

4 Legen Sie als Einkapselungsverfahren die PPP-Einkapselung fest.

```
Encaps=PPP
```

5 Öffnen Sie das Untermenü „Encaps Options“.

6 Setzen Sie den Parameter „Send Auth“ auf „CHAP“ oder „PAP“.

Beispiel:

```
Send Auth=CHAP
```

Das angegebene Protokoll muß von beiden Seiten der Verbindung unterstützt werden.

7 Geben Sie im Parameter „Send PW“ das Kennwort an, das die Pipeline an das entfernte Gerät senden soll.

```
Send PW=*SECURE*
```

8 Geben Sie im Parameter „Recv PW“ das Kennwort an, das das entfernte Gerät an die Pipeline sendet.

```
Recv PW=*SECURE*
```

9 Geben Sie, falls gewünscht, an, welche Datenkomprimierung verwendet werden soll.

Beispiel:

```
Link Comp=Stac
VJ Comp=Yes
```

10 Schließen Sie das Verbindungsprofil.

Konfigurieren einer MP- oder MP+-Verbindung

Sowohl MP- als auch MP+-Verbindungen verwenden für Mehrkanalrufe die PPP-Einkapselung. Die Pipeline unterstützt MP nur als Ausweichmöglichkeit,

wenn MP+ nicht verwendet werden kann, da MP+ viel flexibler bei der Hinzufügung von Kanälen zu einem Ruf arbeitet.

Alle Ascend-Einheiten unterstützen MP+, so daß MPP-Verbindungen zwischen der Pipeline und einer anderen Ascend-Einheit das Protokoll MP+ verwenden. Mit MP+ ist die Pipeline in der Lage, die Bandbreite je nach Bedarf zu erhöhen bzw. zu verringern. Dieses Leistungsmerkmal wird „dynamische Bandbreitenzuweisung“ (Dynamic Bandwidth Allocation, DBA) genannt.

Andere Geräte unterstützen u. U. nur MP, jedoch nicht MP+. Wenn Sie also eine MPP-Verbindung zwischen der Pipeline und einem Gerät konfigurieren, das nicht von Ascend stammt, wird zunächst das Protokoll MP+ angefordert. Kann die Verbindung nicht mit MP+ aufgebaut werden, verwendet die Pipeline statt dessen das Protokoll MP. MP unterstützt zwar Mehrkanalverbindungen, jedoch nicht DBA. Die Anzahl der Kanäle einer MP-Verbindung kann also nicht geändert werden. Außerdem müssen für eine MP-Verbindung alle Kanäle in der Verbindung dieselbe Telefonnummer nutzen (d. h., daß sich die Kanäle auf der antwortenden Seite der Verbindung in einer Mehrfach-Weiterschaltungsgruppe befinden müssen).

Hinweis: Wenn das antwortende Gerät sowohl MP+ als auch MP ablehnt, baut die Pipeline einen PPP-Ruf auf einem einzigen Kanal auf.

Zur Konfiguration einer MP+-Verbindung müssen die folgenden Hauptschritte ausgeführt werden:

- Ermitteln, mit welcher Netzwerksoftware und Ascend-Konfiguration auf der anderen Seite der Verbindung gearbeitet wird
- Ermitteln der erforderlichen Routing-/Bridging- und Authentifizierungsinformationen für die rufende Seite
- Konfigurieren der MP+-Verbindung in einem Verbindungsprofil
- Konfigurieren der Routing- bzw. Bridging-Einstellungen in der Pipeline und für die WAN-Verbindung

Hinweis: Dieser Abschnitt konzentriert sich auf die Konfiguration von MP+-Verbindungen. Dabei wird davon ausgegangen, daß das Antwortprofil so eingerichtet wurde, daß diese Verbindungen zugelassen werden (siehe „Das Antwortprofil“ auf Seite 5-8). Nähere Informationen zur Konfiguration von Routing- und Bridging-Verbindungen entnehmen Sie bitte den entsprechenden Kapiteln weiter hinten in diesem Handbuch.

Dynamische Bandbreitenzuweisung (DBA)

Die dynamische Bandbreitenzuweisung (Dynamic Bandwith Allocation, DBA) ist eine Methode, mit der Kanäle je nach Bedarf automatisch hinzugefügt oder abgezogen werden können. Bei zunehmendem Verkehr fügt die Pipeline dem Ruf gewählte Kanäle hinzu. Geht der Verkehr wieder zurück, werden Kanäle abgezogen und somit Bandbreite freigesetzt, die anderweitig zugewiesen werden kann.

Funktionsweise der DBA

Auf der Grundlage einer bestimmten Zeitspanne wird die mittlere Leitungsnutzung (Average Line Utilization, ALU) berechnet und mit dem Zielgrenzwert verglichen. Wenn die ALU den Grenzwert während der angegebenen Zeitspanne überschreitet, versucht die Pipeline Kanäle hinzuzufügen. Fällt die ALU während der angegebenen Zeitspanne unter den Grenzwert, versucht die Pipeline Kanäle abzuziehen.

Welcher Algorithmus für die Berechnung der ALU während des im Parameter „Sec History“ angegebenen Zeitraums verwendet werden soll, wird mit dem Parameter „Dyn Alg“ festgelegt.

Abbildung 5-1 zeigt die Unterschiede zwischen den verschiedenen Algorithmen.

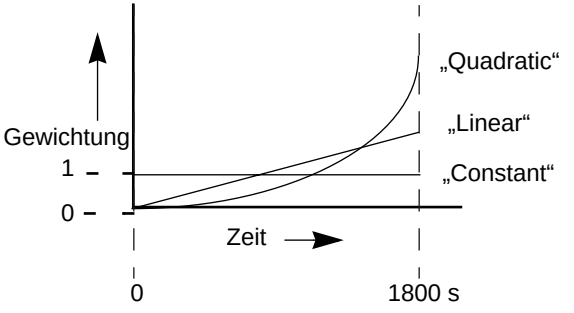


Abbildung 5-1: Bandbreitenalgorithmen für MP+-Rufe

- „Linear“ gibt den letzten Abtastwerten der Bandbreitennutzung mehr Gewicht als den älteren Abtastwerten, die während des im Parameter „Sec

History“ angegebenen historischen Zeitabschnitts ermittelt wurden; die Gewichtung steigt linear an.

- „Quadratic“ (Standardeinstellung für MP+-Rufe) gibt den letzten Abtastwerten der Bandbreitennutzung mehr Gewicht als den älteren Abtastwerten, die während des im Parameter „Sec History“ angegebenen historischen Zeitabschnitts ermittelt wurden; die Gewichtung steigt quadratisch an.
- „Constant“ gibt allen Abtastwerten, die während des im Parameter „Sec History“ angegebenen historischen Zeitabschnitts ermittelt wurden, das gleiche Gewicht. Wenn Sie diese Option wählen, haben die älteren Abtastwerte genauso viel Einfluß auf die Entscheidung, die Bandbreitenzuweisung zu ändern, wie die zuletzt ermittelten Abtastwerte.

Die Pipeline vergleicht die berechnete ALU mit dem im Parameter „Target Util“ angegebenen Parameter. Zur Entscheidung, wann Kanäle hinzugefügt werden sollen, wird die folgende Logik verwendet:

Wenn ALU für > „Add Pers“ Sekunden > „Target Util“, sind + „Inc Ch Count“ Kanäle hinzuzufügen.

Wird der „Target Util“-Grenzwert länger als die im Parameter „Add Pers“ angegebene Zeitspanne überschritten, fügt die Pipeline die im Parameter „Inc Ch Count“ angegebene Zahl von Kanälen hinzu. (Die Kanäle müssen verfügbar sein, und es werden maximal so viele Kanäle hinzugefügt, wie im Parameter „Max Ch Count“ angegeben sind. Damit mehrere Kanäle gleichzeitig hinzugefügt werden können, muß im Parameter „Parallel Dial“ ein Wert größer als 1 festgelegt werden.)

Zur Entscheidung, wann Kanäle abgezogen werden sollen, verwendet die Pipeline die folgende Logik:

Wenn ALU für > „Sub Pers“ Sekunden < „Target Util“, sind – „Dec Ch Count“ Kanäle abzuziehen.

Wenn die ALU länger als im Parameter „Sub Pers“ angegeben unter den „Target Util“-Grenzwert fällt, zieht die Pipeline die im Parameter „Dec Ch Count“ angegebene Zahl von Kanälen ab. (Dabei wird jedoch niemals der Basiskanal der Verbindung entfernt noch kann die Anzahl der Kanäle unter den im Parameter „Min Ch Count“ festgelegten Wert fallen. Es werden auch niemals so viele Kanäle entfernt, daß die ALU den „Target Util“-Wert überschreitet.)

Einzelheiten zum Entfernen des Basiskanals der Verbindung aufgrund geringerer Bandbreitenerfordernisse können Sie dem Abschnitt „Beenden eines Anrufs aufgrund von ungenutzter Bandbreite“ auf Seite 5-21 entnehmen. Welches Verfahren empfohlen wird, eine Verbindung zu beenden, die über einen bestimmten Zeitraum hinweg inaktiv ist, erfahren Sie in „Überblick über die Sitzungsoptionen“ auf Seite 5-12.

Richtlinien für die Konfiguration der DBA

Um die MP+-Verbindung optimal nutzen zu können, müssen die folgenden Parameter auf beiden Seiten der Verbindung die gleichen Werte haben:

- „Base Ch Count“ (im Verbindungsprofil)
- „Min Ch Count“ (im Antwortprofil und im Verbindungsprofil)
- „Max Ch Count“ (im Antwortprofil und im Verbindungsprofil)

Bei der Konfiguration der Parameter für die dynamische Bandbreitenzuweisung sind die folgenden zusätzlichen Empfehlungen zu beachten:

- Die Werte für die Parameter „Sec History“, „Add Pers“ und „Sub Pers“ sollten Spitzen bei der Bandbreitennutzung ausgleichen, die kürzer andauern, als das Hinzufügen von Kapazität möglich ist.

  Über ISDN-Leitungen kann die Pipeline Bandbreite in weniger als fünf Sekunden hinzufügen.
- Wenn die Pipeline Bandbreite hinzufügt, fällt im Normalfall eine Mindestnutzungsgebühr an. Danach wird zeitabhängig abgerechnet.

  Der Wert des Parameters „Sub Pers“ sollte mindestens der Mindestnutzungsdauer plus einer oder zwei Gebühreneinheiten entsprechen. Häufig werden die Gebühren für das nächste Vielfache von sechs Sekunden berechnet, wobei für die ersten dreißig Sekunden eine Mindestgebühr anfällt. Einzelheiten zur Gebührenstruktur für vermittelte Gespräche erfahren Sie von Ihrer Telefongesellschaft.
- Vermeiden Sie es, Kanäle zu schnell hinzuzufügen oder abzuziehen (Abstände von weniger als 10–20 Sekunden).

  Durch das zu schnelle Hinzufügen oder Abziehen von Kanälen entstehen viele Kurzzeitanrufe, die jeweils extra berechnet werden. Außerdem kann dadurch die Verbindungseffektivität beeinträchtigt werden, da die Geräte auf beiden Seiten der Verbindung Daten erneut übertragen müssen, wenn sich die Verbindungsgeschwindigkeit ändert.

DBA-Überwachung

Mit Hilfe des Parameters „DBA Monitor“ können Sie festlegen, welche Seite der Verbindung den Verkehr überwachen soll. Das Hinzufügen oder Abziehen von Kanälen kann jedoch nur von der Seite aus erfolgen, die den Ruf initiiert hat.

Standardmäßig wird Bandbreite auf der Grundlage der Menge der von der rufenden Seite gesendeten Daten hinzugefügt bzw. abgezogen. Um dieses Verhalten zu ändern, können Sie den Parameter „DBA Monitor“ auf „Transmit-Recv“ einstellen, wodurch das rufende Gerät angewiesen wird, bei der Zuweisung bzw. dem Abziehen von Bandbreite sowohl die gesendeten als auch die empfangenen Daten zu berücksichtigen. Wird statt dessen der Wert „None“ festgelegt, erfolgt keinerlei Überwachung des Verkehrs durch die Pipeline. Wenn der Parameter „DBA Monitor“ auf beiden Seiten der Verbindung den Wert „None“ hat, ist die dynamische Bandbreitenzuweisung deaktiviert.

Beenden eines Anrufs aufgrund von ungenutzter Bandbreite

Im Parameter „Idle Pct“ kann ein Wert für die Bandbreitennutzung (in Prozent) angegeben werden, bei dessen Unterschreitung MP+-Rufe beendet werden. Die Bandbreitennutzung muß *auf beiden Seiten der Verbindung* unter diesen Wert fallen, bevor die Pipeline den Ruf beendet. Hat das Gerät am entfernten Ende der Verbindung einen niedrigeren „Idle Pct“-Wert als Ihre Pipeline, wird der Ruf erst dann beendet, wenn die Bandbreitennutzung unter den niedrigeren der beiden Werte fällt.

Der Standardwert für „Idle Pct“ ist „0“. Bei diesem Wert ignoriert die Pipeline die Bandbreitennutzung, wenn es darum geht, einen Ruf zu beenden und statt dessen den „Idle“-Timer zu verwenden.

Beispiel für eine MP+-Konfiguration

Tabelle 5-4 zeigt die Parameter, die in Zusammenhang mit MP+-Verbindungen verwendet werden können.

Tabelle 5-4: MP+-Parameter

Ort	**Parameter**
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Encaps=MPP
Ethernet > Connections > *alle Profile* > Encaps options...	Send Auth=CHAP Send PW=*SECURE* Aux Send PW=N/A Recv PW=*SECURE* DBA Monitor=Transmit Base Ch Count=1 Min Ch Count=1 Max Ch Count=1 Inc Ch Count=1 Dec Ch Count=1 MRU=1524 LQM=No LQM Min=600 LQM Max=600 Link Comp=Stac VJ Comp=Yes Dyn Alg=Quadratic Sec History=15 Add Pers=5 Sub Pers=10 Target Util=70 Idle Pct=0

Bei MP+-Rufen können Sie für den Grundkanal des Rufes und für die zusätzlich zugewiesenen Kanäle jeweils unterschiedliche Authentifizierungsverfahren (Kennwörter) verwenden. Siehe dazu Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Zum Festlegen des Namens für die Pipeline ist wie folgt vorzugehen:

1 Öffnen Sie das Systemprofil.

2 Geben Sie im Parameter „Name“ einen Namen für die Pipeline-Einheit an.
Beispiel:

```
Name=PIPE1
```

Für diesen Parameter muß ein Wert festgelegt werden, wenn „Send Auth= PAP“ oder „Send Auth=CHAP“ festgelegt wurde.

3 Schließen Sie das Systemprofil.

Konfigurieren einer MP+-Verbindung:

1 Öffnen Sie das Verbindungsprofil.

2 Geben Sie im Parameter „Station“ den Namen des entfernten Geräts an.
Beispiel:

```
Station=andereseite
```

Beachten Sie, daß der Name genau eingegeben werden muß, einschließlich aller Groß- bzw. Kleinbuchstaben, Leerzeichen bzw. Unterstriche.

3 Aktivieren Sie das Profil.

```
Active=Yes
```

4 Legen Sie als Einkapselungsverfahren die MP+-Einkapselung fest.

```
Encaps=MPP
```

5 Öffnen Sie das Untermenü „Encaps Options“.

6 Geben Sie an, welches Authentifizierungsprotokoll verwendet werden soll.
Beispiel:

```
Send Auth=CHAP
```

7 Geben Sie im Parameter „Send PW“ das Kennwort an, das die Pipeline an das entfernte Gerät senden soll.

```
Send PW=*SECURE*
```

8 Geben Sie im Parameter „Recv PW“ das Kennwort an, das das entfernte Gerät an die Pipeline sendet.

```
Recv PW=*SECURE*
```

9 Legen Sie die Zahl der Kanäle fest, die die Pipeline für diese Verbindung nutzen kann.
Beispiel:

```
Base Ch Count=1
Min Ch Count=1
Max Ch Count=3
```

10 Schalten Sie, falls gewünscht, die Datenkomprimierung ein.

Beispiel:

```
Link Comp=Stac
VJ Comp=Yes
```

11 Konfigurieren Sie die Bandbreitenoptionen.

Beispiel:

```
Dyn Alg=Quadratic
Sec History=15
Add Pers=5
Sub Pers=10
Target Util=70
```

Näheres dazu finden Sie im Abschnitt „Dynamische Bandbreitenzuweisung (DBA)“ auf Seite 5-18.

12 Legen Sie einen Wert für den Parameter „Idle Pct“ fest.

Beispiel:

```
Idle Pct=0
```

Wird dieser Parameter auf „0“ gesetzt, wird statt dessen der Parameter „Idle“ verwendet.

13 Schließen Sie das Verbindungsprofil.

MPP-Festverbindungen

Eine MPP-Festverbindung („Nailed/MPP“) ist eine permanente Verbindung, der gewählte Kanäle hinzugefügt werden können, um die zur Verfügung stehende Bandbreite zu erweitern. „Nailed/MPP“-Verbindungen werden aufgebaut, wenn die festgeschalteten bzw. gewählten Kanäle Ende-zu-Ende verbunden werden.

Die Hinzufügung bzw. das Abziehen von gewählten Kanälen erfolgt auf der Grundlage der Einstellung des Parameters „DBA“ im Verbindungsprofil einer der beiden Seiten der Verbindung. Wenn die beiden Seiten einer Verbindung keine Übereinkunft über die Anzahl der Kanäle erzielen können, die für eine Verbindung benötigt werden, gilt der größere der beiden Werte. Die Berechnung der erforderlichen Bandbreite erfolgt durch beide Seiten auf der Grundlage des jeweils empfangenen Verkehrs.

Die Höchstzahl der Kanäle für eine MPP-Festverbindung wird entweder durch den Wert des Parameters „Max Ch Count“ oder die Anzahl der festgeschalteten Kanäle in der angegebenen Gruppe bestimmt, je nachdem, welcher dieser Werte größer ist. Fällt ein festgeschalteter Kanal aus, wird dieser durch einen gewählten Kanal ersetzt, auch dann, wenn der Ruf mit mehr als der Mindestzahl von Kanälen online ist.

Zur Konfiguration einer MPP-Festverbindung muß zunächst eine reguläre MP+-Verbindung konfiguriert werden. Anschließend sind die folgenden Schritte auszuführen:

1 Öffnen Sie das Untermenü „Telco options“ des Verbindungsprofils.

2 Geben Sie für den Parameter „Call Type“ den Wert „Nailed/Mpp“ ein.

```
Call Type=Nailed/Mpp
```

3 Geben Sie die Gruppennummer der festgeschalteten Kanäle an.

Beispiel:

```
Group=1,2
```

4 Geben Sie an, daß die Pipeline als einziger Anrufer für den vermittelten Teil der Verbindung in Frage kommt.

Beispiel:

```
AnsOrig=Call Only
FT1 Caller=Yes
```

5 Schließen Sie das Verbindungsprofil.

Auf der anderen Seite der Verbindung sind die Parameter „AnsOrig“ und „FT1 Caller“ so einzustellen, daß Rufe nur beantwortet werden. Beachten Sie, daß der Befehl „DO HANGUP“ nur von der rufenden Seite der Verbindung aus gegeben werden kann.

Sie können die Parameter einer „Nailed/MPP“-Verbindung jederzeit neu konfigurieren. Dabei ist jedoch zu beachten, daß die Änderungen immer erst nach der Beendigung und dem erneuten Aufbau des Rufes wirksam werden. Wenn Sie jedoch dem Parameter „Group“ einen Wert hinzufügen und die Änderung speichern, werden die zusätzlichen Kanäle der Verbindung hinzugefügt, ohne daß diese dazu beendet und erneut aufgebaut werden muß. Dies gilt zum Beispiel für das Wechseln von „Group=1“ zu „Group= 2“.

Hinweis: Wenn eine „Nailed/MPP“-Verbindung unterbrochen ist und auch die festgeschalteten Kanäle nicht verbunden sind, stellt sich die Verbindung erst wieder selbst her, wenn die festgeschalteten Kanäle wieder online sind oder die gewählten Kanäle gewählt werden. (Die gewählten Kanäle werden gewählt, wenn die rufende Einheit ein Paket empfängt, dessen Ziel die Einheit auf der anderen Seite der „Nailed/MPP“-Verbindung ist.)

Konfigurieren von Frame-Relay-Verbindungen

Frame-Relay-Profile dienen zur Definition einer Verbindung zwischen der Pipeline und einem Frame-Relay-Switch. Obgleich es zwar möglich ist, eine gewählte Verbindung in einem Frame-Relay-Profil zu konfigurieren, ist diese Art von Verbindung so gut wie immer eine Festverbindung. Gewählte Verbindungen können nur in den seltenen Fällen verwendet werden, in denen das Frame-Relay-Netzwerk Einwählverbindungen zuläßt und Verbindungen zum Netzwerk immer durch die Pipeline initiiert werden. (Frame-Relay-Vermittlungsstellen unterstützen z. Z. keine abgehenden Verbindungen.)

Verbindungsprofile dienen zur Definition einer logischen Verbindung zu einem Endpunkt im Frame-Relay-Netzwerk. In jedem Verbindungsprofil muß ein DLCI (Data Link Connection Identifier) für diese Verbindung angegeben werden. Ein DLCI ist eine Zahl zwischen 16 und 991, die vom Frame-Relay-Administrator festgelegt wird. DLCIs sind keine Adressen, sondern lokale Labels zur Kennzeichnung einer logischen Verbindung zwischen einem Gerät und einem Frame-Relay-Switch. Der Switch verwendet die DLCIs zum Routing von Rahmen durch das Netzwerk. Beim Durchlaufen der Frames durch mehrere Vermittlungsstellen können sich die DLCIs jeweils ändern.

Hinweis: Zur Definition einer logischen Verbindung zum Frame-Relay-Netzwerk brauchen Sie mindestens ein Frame-Relay-Profil und ein Verbindungsprofil.

Zur Konfiguration einer Frame-Relay-Verbindung sind die folgenden Hauptschritte auszuführen:

- Überprüfen, ob festgeschaltete Kanäle für die Verbindung zum Frame-Relay-Switch zur Verfügung stehen
- Konfigurieren eines Frame-Relay-Profils, das diese Kanäle für die Verbindung mit dem FR-Switch verwendet
- Ermitteln der benötigten DLCIs in Zusammenarbeit mit dem Frame-Relay-Administrator

  Für jede Verbindung wird ein eigener DLCI benötigt.
- Ermitteln der erforderlichen Routing- bzw. Bridging-Informationen in Zusammenarbeit mit der entfernten Seite
- Überprüfen, ob im Antwortprofil die FR-Einkapselung festgelegt wurde
- Konfigurieren der Frame-Relay-Verbindung in einem Verbindungsprofil
- Konfigurieren der Routing- bzw. Bridging-Einstellungen in der Pipeline und über die WAN-Verbindung

Hinweis: Dieser Abschnitt befaßt sich mit der Konfiguration von Frame-Relay-Verbindungen. Dabei wird davon ausgegangen, daß das Antwortprofil für diese Art von Verbindungen eingerichtet wurde (siehe „Das Antwortprofil“ auf Seite 5-8). Einzelheiten zur Konfiguration der Routing- und Bridging-Werte entnehmen Sie bitte den entsprechenden Kapiteln weiter hinten in diesem Handbuch.

Vorbereitung

Einige Ascend-Einheiten unterstützen als Option Frame Relay. Wenn Sie sich nicht sicher sind, ob Ihre Einheit Frame Relay unterstützt, gehen Sie mit Hilfe der Tabulatortaste zum Statusfenster „Sys Option“, und suchen Sie dort mit Hilfe der Pfeiltasten (bzw. durch Drücken von Strg-N) nach dem folgenden Eintrag:

```
Frm Rel Installed
```

Wenn Sie diesen Eintrag finden, ist Frame Relay installiert.

Setzen Sie sich dann mit Ihrem Frame-Relay-Administrator in Verbindung, und fragen Sie ihn nach den DLCIs. Diese DLCIs versetzen den Frame-Relay-Switch in die Lage herauszufinden, welche logische Verbindung mit den einzelnen Verbindungsprofilen assoziiert ist.

Optionen für die Konfiguration von logischen Verbindungen

In einem Verbindungsprofil wird eine logische Verbindung zu einem Endpunkt definiert, zu dem Sie über einen Frame-Relay-Switch gelangen. Die Pipeline unterstützt den Frame-Relay-„Gateway“-Modus. Eine Frame-Relay-Gateway-Verbindung ist eine Bridging- bzw. Routing-Verbindung zwischen der Pipeline und einem entfernten Gerät über einen Frame-Relay-Switch. Wenn die Pipeline IP-Pakete für dieses Gerät empfängt, kapselt sie diese mit Hilfe des Frame-Relay-Einkapselungsverfahrens (RFC 1490) ein und leitet den Datenstrom unter Verwendung des angegebenen DLCI an den Frame-Relay-Switch weiter. Der Frame-Relay-Switch verwendet den DLCI zum Routing der Rahmen zu deren eigentlichem Ziel.

Abbildung 5-2 zeigt eine Pipeline mit drei Gateway-Verbindungen zu entfernten Geräten über das Frame-Relay-Netzwerk. Gateway-Verbindungen können Bridging und Routing unterstützen, so daß die Pipeline jede Art von Protokollverkehr vom lokalen Netzwerk aus zum Frame-Relay-Netzwerk weiterleiten kann.

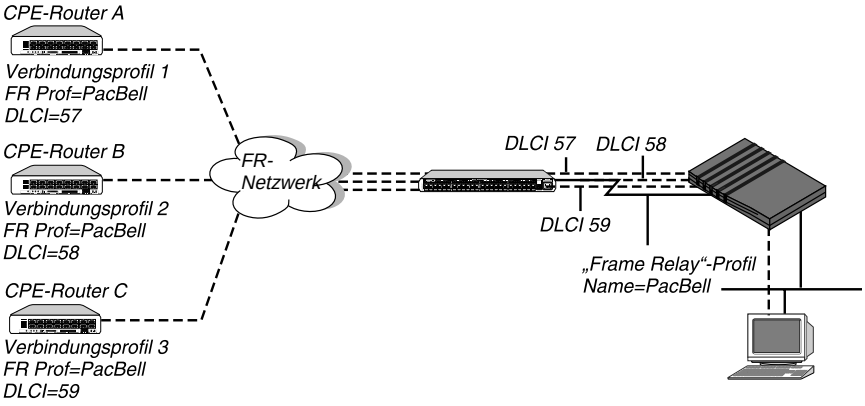


Abbildung 5-2: Gateway-Verbindungen zum Frame-Relay-Netzwerk

Die Verbindungsprofile 1, 2 und 3 verwenden die Frame-Relay-Einkapselung (RFC 1490) und enthalten sowohl eine DLCI-Nummer für die logische Verbindung als auch den Namen des Frame-Relay-Profils für die festverbindung. Das Frame-Relay-Profil 1 definiert eine Festverbindung zwischen der Pipeline und einem Frame-Relay-Switch. Die Verbindungsprofile und das Frame-Relay-Profil in diesem Beispiel werden im folgenden erklärt:

Verbindungsprofile (Gateway)

```
20-101
Station=CPEA
Active=Yes
Encaps=FR
Encaps options...
   FR Prof=PacBell
   DLCI=57

20-102
Station=CPEB
Active=Yes
Encaps=FR
Encaps options...
   FR Prof=PacBell
   DLCI=58

20-103
Station=CPEC
Active=Yes
Encaps=FR
Encaps options...
   FR Prof=PacBell
   DLCI=59
```

Frame-Relay-Profil

```
20-501 PacBell
Name=PacBell
Active=Yes
Call Type=Nailed
Nailed Grp=1
Data Svc=64K
Link Mgmt=T1.617D
...
```

Beispiel für ein Frame-Relay-Profil

Tabelle 5-5 zeigt die Konfigurationsparameter, die für den Aufbau einer Festverbindung zum Frame-Relay-Switch benötigt werden.

Tabelle 5-5: Parameter im Frame-Relay-Profil

Ort	Parameter mit Beispielwerten
Ethernet > Frame Relay > Frame-Relay-Profil	Name=PacBell7 Active=Yes Call Type=Nailed Nailed Grp=1 Data Svc=64k Dial #=N/A Link Mgmt=T1.617D N391=6 N392=3 N393=4 T391=10 T392=15 MRU=1532

Definition des Frame-Relay-Profils:

1 Öffnen Sie ein Frame-Relay-Profil, und weisen Sie ihm einen Namen zu.

Beispiel:

```
Name=PacBell
```

Der Name kann bis zu 15 alphanumerische Zeichen enthalten. Dieser Name wird in Verbindungsprofilen verwendet, die diese Verbindung zum Switch benutzen.

2 Aktivieren Sie das Profil.

```
Active=Yes
```

3 Geben Sie an, daß es sich hierbei um eine Festverbindung handelt, und welche Gruppennummer der festgeschalteten Kanäle (bzw. welche serielle WAN-Schnittstelle) verwendet werden soll.

Beispiel:

```
Call Type=Nailed
Nailed Grp=1
```

Für Frame-Relay-Verbindungen ist „Nailed“ der Standardwert. Wenn der Parameter „Call Type“ diesen Wert hat, sind die anderen telefongesellschaftsspezifischen Parameter nicht verfügbar („N/A“). Wenn der Frame-Relay-Switch auch Einwählverbindungen zuläßt, können Sie auch den Wert „Switched“ wählen. Frame-Relay-Netzwerke unterstützen gegenwärtig jedoch keine abgehenden Verbindungen.

4 Legen Sie den Datendienst fest.

Beispiel:

```
Data Svc=64k
```

5 Geben Sie an, welches Verbindungsmanagement-Protokoll zwischen der Pipeline und dem Frame-Relay-Switch verwendet werden soll.

Beispiel:

```
Link Mgmt=T1.617D
```

Wird „Link Mgmt=T1.617D“ festgelegt, sind auch die folgenden Parameter festzulegen:

```
N391
N392
N393
T391
T392
```

„N391“ gibt an, wie viele Abfragezyklen die Pipeline wartet, bevor sie einen vollständigen Statusbericht anfordert. „N392“ gibt die Höchstzahl der Fehlerereignisse an, die im gleitenden Fenster auftreten können, das durch „N393“ definiert wird. „N393“ gibt die Breite des gleitenden Fensters an, das vom Parameter „N392“ genutzt wird.

„T391“ gibt an, wie viele Sekunden zwischen Statusabfragemeldungen liegen sollen, und „T392“ gibt an, wie viele Sekunden die Pipeline auf eine Statusabfragemeldung wartet, bevor sie einen Fehler aufzeichnet.

Nähere Informationen zu diesen Parametern finden Sie im *Referenzhandbuch*.

6 Schließen Sie das Frame-Relay-Profil.

Beispiel für eine Gateway-Verbindung

Tabelle 5-6 zeigt die Verbindungsprofil-Parameter für Frame-Relay-Gateway-Verbindungen.

Tabelle 5-6: Parameter für Frame-Relay-Gateway-Verbindungen

Ort	Parameter
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Encaps=FR
Ethernet > Connections > *alle Profile* > Encaps options...	FR Prof=Pac Bell DLCI=17

Hinweis: In diesem Abschnitt wird nur die Konfiguration der Frame-Relay-Einstellungen beschrieben. Routing- und Bridging-Parameter müssen ebenfalls konfiguriert werden, damit die Verbindung funktionstüchtig ist.

Zur Konfiguration einer Frame-Relay-Gateway-Verbindung zu einem entfernten Gerät im Frame-Relay-Netzwerk ist wie folgt vorzugehen:

1. Öffnen Sie ein Verbindungsprofil, und geben Sie den Namen des entfernten Geräts an.

   Beispiel:

   ```
   Station=ENTFA
   ```

2. Aktivieren Sie das Profil.

   ```
   Active=Yes
   ```

3. Wählen Sie als Einkapselungsverfahren die Frame-Relay-Einkapselung.

   ```
   Encaps=FR
   ```

   Die Pipeline kapselt Pakete mit Hilfe dieses Einkapselungsverfahrens ein, bevor sie sie weiterleitet. Ankommende Pakete vom entfernten Gerät werden mit diesem Einkapselungsverfahren von ihrer Einkapselung „befreit“.

4. Öffnen Sie das Untermenü „Encaps Options“.

5. Geben Sie als Wert für den Parameter „DLCI“ die Nummer ein, die Sie vom Frame-Relay-Administrator erhalten haben.

Beispiel:

```
DLCI=500
```

Diese Nummer, die vom Frame-Relay-Administrator zugewiesen wird, gibt an, wie Pakete am Frame-Relay-Switch „geroutet“ werden.

6 Geben Sie den Namen des Frame-Relay-Profils an, in dem die Festverbindung zum Frame-Relay-Switch definiert ist.

Beispiel:

```
FR Prof=PacBell
```

Der Name muß mit dem Wert des Parameters „Name“ im Frame-Relay-Profil genau übereinstimmen (auch auf Groß- und Kleinschreibung achten!).

7 Schließen Sie das Verbindungsprofil.

Konfigurieren des seriellen WAN-Anschlusses

Sie können den Terminal-Anschluß auf der Rückseite der Pipeline als eigens für das WAN bestimmten Anschluß verwenden.

Hinweis: Die Nutzung des Terminal-Anschlusses als serielle WAN-Schnittstelle ist nur bei Pipeline-Einheiten möglich, bei denen sich an der Rückseite ein kleiner Schalter befindet.

Wenn die serielle WAN-Schnittstelle aktiviert ist, werden sämtliche Verbindungsprofile alle 10 Sekunden überprüft. Ist ein Verbindungsprofil für den Mietleitungsbetrieb konfiguriert und der Parameter „Nailed Group“ in diesem Profil auf „3“ eingestellt, wird der Terminal-Anschluß für den synchronen HDLC-Modus programmiert, und es wird versucht, die Verbindung über diesen Anschluß aufzubauen.

Die Datenübertragungsrate der seriellen WAN-Schnittstelle wird durch die von der Verbindung empfangene Taktrate bestimmt. Der Höchstwert ist 8 MBit/s. Die Taktrate an der seriellen WAN-Schnittstelle hat keinerlei Auswirkungen auf die Bandbreite anderer WAN-Schnittstellen in der Pipeline.

Bei der Konfiguration des „Serial WAN“-Profils müssen Sie festlegen, welcher Frame-Relay- oder anderer Verbindungstyp die serielle WAN-Schnittstelle nutzen soll.

Hinweis: Das Zeichengabeprotokoll für die serielle WAN-Schnittstelle ist V.35. Die elektrische Schnittstelle entspricht RS-232. Daher muß das elektrische Signal von RS-232 zu V.35 umgewandelt werden.

Zur Festlegung, das der Terminal-Anschluß als serieller WAN-Anschluß verwendet werden soll, ist wie folgt vorzugehen:

1 Stellen Sie den Schalter für den seriellen WAN-Anschluß auf die Position „On“.

Welche Position das im Einzelfall ist, hängt vom jeweiligen Pipeline-Modell ab:

– Ist der Schalter horizontal angebracht, ist die „On“-Position die Position, in der der Schalter vom Terminal-Anschluß wegzeigt (siehe Abbildung 5-3).

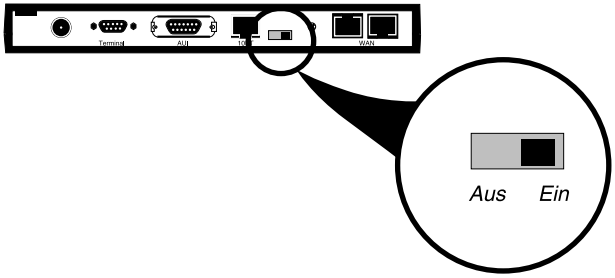


Abbildung 5-3: „On“-Position für den Schalter zur Aktivierung des seriellen WAN-Anschlusses

Wenn der Schalter vertikal angebracht ist, ist die „On“-Position die untere Position.

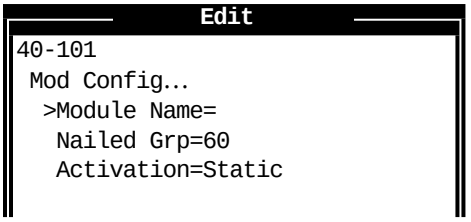
2 Legen Sie im Menü „Sys Config“ für den Parameter „Switch Usage“ den Wert „Serial WAN“ fest.

3 Schließen Sie das Anschlußkabel für den seriellen WAN-Anschluß an Ihre WAN-Schnittstelle an.

4 Setzen Sie die Pipeline zurück.

Sobald die Pipeline wieder hochgefahren ist, ist der serielle WAN-Anschluß aktiv.

5 Öffnen Sie das „Serial WAN“-Profil.



6 Weisen Sie dem seriellen WAN-Anschlußmodul einen Modulnamen zu (optional).

7 Geben Sie einen Wert für den Parameter „Nailed Grp“ ein.

Beispiel:

```
Nailed Grp=3
```

Die Gruppennummer, die Sie hier eingeben, muß mit dem Wert des Parameters „Nailed Grp“ im Frame-Relay-Profil bzw. Verbindungsprofil übereinstimmen, das den Transport der Pakete über die serielle WAN-Schnittstelle übernimmt. Es darf keine Gruppennummer angegeben werden, die bereits für eine Festverbindung an einer anderen Schnittstelle verwendet wird.

8 Legen Sie einen Wert für den Parameter „Activation“ fest.

Beispiel:

```
Activation=Static
```

Dieser Parameter gibt an, welche Signale den Datenfluß über den seriellen WAN-Anschluß steuern. Der Wert hängt vom DCE ab, mit dem der serielle WAN-Anschluß verbunden ist.

9 Schließen Sie das „Serial WAN“-Profil.

Konfigurieren der Pipeline als Bridge

6

Dieses Kapitel enthält die folgenden Abschnitte:

Die Pipeline als Bridge – Einführung

Dieser Abschnitt bietet einen Überblick über das Paket-Bridging und beschreibt, wie die Pipeline beim Aufbau einer Bridging-Verbindung vorgeht.

In der Pipeline werden Bridges dazu benutzt, Netzwerke bzw. Netzwerksegmente miteinander zu verbinden, wenn andere Protokolle als IP und IPX, wie z. B. AppleTalk, zum Einsatz kommen, obgleich es auch möglich ist, Bridging für die Verbindung von Segmenten eines IP- oder IPX-Netzwerks einzusetzen. Da Bridging-Verbindungen die Pakete auf der Hardware-Adressenebene („Link Layer“ oder „Datensicherungsschicht“) weiterleitet, wird nicht zwischen den Protokollarten unterschieden, so daß keine protokollspezifische Netzwerkkonfiguration erforderlich ist.

Hinweis: Außer den Geschwindigkeitsvorteilen, die das Routing bietet, haben Router auch noch andere Vorteile gegenüber Bridges. Da sie Pakete auf der „Network Layer“ („Netzwerkschicht“) überprüfen, kann die Filterung logischer Adressen veranlaßt und somit die Sicherheit und Kontrolle erhöht werden. Außerdem unterstützen Router die Verwendung mehrerer Übertragungswege zu einem bestimmten Ziel, wodurch eine höhere Zuverlässigkeit und Geschwindigkeit der Paketzustellung erreicht wird.

Bridging wird in der Pipeline vor allem zu den folgenden Zwecken eingesetzt:

- Herstellung von Verbindungen mittels Protokollen, bei denen kein Routing stattfindet
- Verbindung zweier Standorte, so daß deren Knoten zu ein und demselben LAN zu gehören scheinen
- Unterstützung von Protokollen, für deren Funktionieren Broadcasts erforderlich sind, wie z. B. BOOTP

Bridges überprüfen *alle* Pakete im LAN (sogenannter „promiskuitiver Modus“), so daß beim Bridging ein größerer Prozessor- und Speicher-Overhead entsteht als beim Routing. Dieser größere Overhead kann bei stark belasteten Netzwerken zu einer Verlangsamung der Arbeitsgeschwindigkeit führen.

Initiierung einer WAN-Bridging-Verbindung

Wenn die Pipeline für das Bridging konfiguriert wurde, akzeptiert sie alle Pakete im Ethernet, leitet aber nur die Pakete weiter, die eine der folgenden Bedingungen erfüllen:

- das Paket hat eine physikalische Adresse, die nicht zum lokalen Ethernet-Segment gehört (das Segment, mit dem die Pipeline verbunden ist)
- das Paket hat eine Broadcast-Adresse

In Zusammenhang mit Bridging-Verbindungen ist stets zu beachten, daß diese nicht mit logischen (Netzwerk-)Adressen, sondern mit physikalischen und Broadcast-Adressen arbeiten.

Physikalische Adressen und die Bridging-Tabelle

Eine physikalische Adresse ist eine eindeutige Adresse eines bestimmten Netzwerk-Controllers auf der Hardware-Ebene. Die physikalische Adresse eines Geräts wird auch MAC-Adresse (Media Access Control) genannt. Im Ethernet ist die physikalische Adresse eine sechs Byte große Hexadezimalzahl, die vom Hersteller der Ethernet-Hardware festgelegt wird, wie z. B.:

```
0000D801CFF2
```

Wenn die Pipeline ein Paket empfängt, dessen Ziel-MAC-Adresse sich nicht im lokalen Netzwerk befindet, sucht sie diese Adresse zunächst in ihrer internen Bridging-Tabelle (siehe „Transparentes Bridging“ auf Seite 6-10). Findet sie die Ziel-MAC-Adresse des Pakets in der Bridging-Tabelle, wählt die Pipeline die Verbindung und „bridgt“ das Paket.

Ist *kein* Eintrag für diese Adresse in der Bridging-Tabelle enthalten, sucht die Pipeline nach aktiven Sitzungen, bei denen Bridging aktiviert ist. Gibt es eine oder mehrere aktive Verbindungen, über die Bridging möglich ist, leitet die Pipeline das Paket über *alle* aktiven Sitzungen, bei denen Bridging aktiviert ist.

Hinweis: Die Pipeline kann keine Verbindung für Pakete wählen, die sich nicht im lokalen Netzwerk befinden und nicht in ihrer Bridging-Tabelle vertreten sind, da sie keine Möglichkeit hat, das richtige Verbindungsprofil zu finden. Näheres dazu finden Sie im Abschnitt „Verwalten der Bridging-Tabelle“ auf Seite 6-9.

Broadcast-Adressen und der Parameter „Dial Brdcast“

Eine Broadcast-Adresse wird von mehreren Knoten im Netzwerk erkannt. So lautet die Ethernet-Broadcast-Adresse auf der physikalischen Ebene z. B.:

FFFFFFFFFFFF

Pakete mit dieser Zieladresse werden von allen Geräten im selben Netzwerk empfangen. Wurde die Pipeline als Router konfiguriert, werden Broadcast-Pakete abgelehnt. Als Bridge konfiguriert, leitet die Pipeline Pakete mit Broadcast-Zieladressen über alle aktiven Sitzungen weiter, bei denen Bridging aktiviert ist, und sie initiiert eine Sitzung für alle Verbindungsprofile, bei denen der Parameter „Dial Brdcast“ den Wert „Yes“ hat.

Hinweis: ARP-Broadcast-Pakete, die eine in der Bridging-Tabelle eingetragene IP-Adresse enthalten, erfahren eine Sonderbehandlung (siehe dazu „Statische Bridging-Tabelleneinträge“ auf Seite 6-11).

Herstellen einer Bridging-Verbindung durch die Pipeline

Zum Aufbau einer Bridging-Verbindung verwendet die Pipeline Stationsnamen und Kennwörter. Siehe dazu Abbildung 6-1.

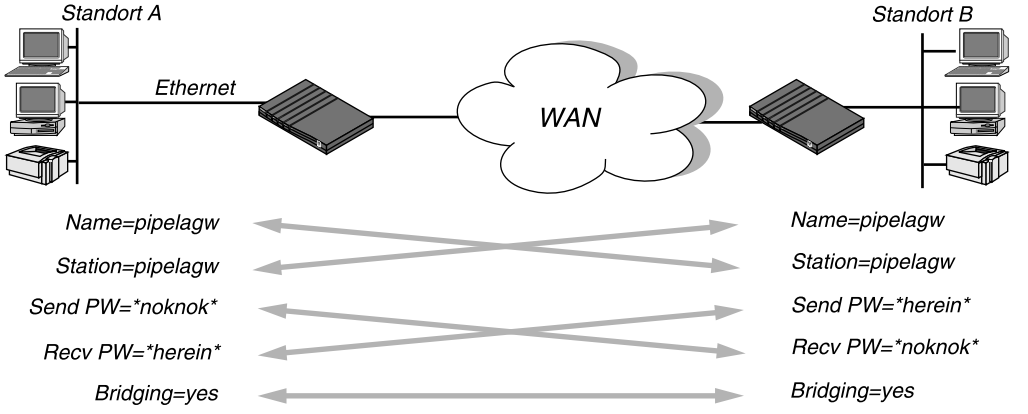


Abbildung 6-1: Aushandeln einer Bridging-Verbindung (PPP-Einkapselung)

Der der Pipeline im Parameter „Name“ des Systemprofils zugewiesene Systemname muß *exakt* mit dem im Verbindungsprofil der entfernten Bridge angegebenen Gerätenamen übereinstimmen (Groß- bzw. Kleinschreibung beachten!). Gleiches gilt für den Namen der entfernten Bridge und den im Parameter „Station“ dieses Verbindungsprofils angegebenen Namen.

Hinweis: Die häufigste Fehlerursache bei der Ersteinrichtung von PPP-Bridging-Verbindungen ist die Angabe eines falschen Namens für die Pipeline oder das entfernte Gerät. Oftmals wird nicht auf die Groß- und Kleinschreibung geachtet, oder es werden Bindestriche, Leerzeichen oder Unterstriche vergessen.

Bridging-Parameter im „Answer“-Profil

Das Bridging muß sowohl auf der antwortenden als auch auf der rufenden Seite einer PPP-, MP- oder MP+-Sitzungsverbindung aktiviert sein, da sonst kein Bridging stattfinden kann. Außerdem ist zur eindeutigen Identifizierung von Geräten die PAP- oder CHAP-Authentifizierung erforderlich. Einzelheiten zur PPP- bzw. MPP-Einkapselung finden Sie im Kapitel 5, „Konfigurieren von WAN-Verbindungen“.

In Tabelle 6-4 werden die Bridging-Parameter im Antwortprofil aufgeführt.

Tabelle 6-1: Bridging-Parameter im Antwortprofil

Ort	Parameter mit Beispielwerten
Ethernet > Answer > PPP options... (Antwortprofil)	Bridge=Yes Recv Auth=Either

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Hinweis: Im Gegensatz zu IP-Routing-Konfigurationen, bei denen die Pipeline das rufende Gerät eindeutig an dessen IP-Adresse erkennt, verfügen Bridging-Konfigurationen nicht über die Möglichkeit, die Quelle ankommender Rufe zu identifizieren. Daher muß mit Kennwort-Authentifizierung mittels PAP oder CHAP gearbeitet werden, es sei denn, im selben Verbindungsprofil ist IP-Routing konfiguriert.

Zum Festlegen der Antwortprofil-Parameter für eine Bridging-Verbindung ist wie folgt vorzugehen:

1. Öffnen Sie das Antwortprofil („Answer“).
2. Öffnen Sie das Untermenü „PPP Options“.
3. Aktivieren Sie das Bridging.

   ```
   Bridge=Yes
   ```

   Hinweis: Der Parameter „Bridge“ ist nicht verfügbar („N/A“), wenn der Parameter „Bridging“ in „Ethernet-->Mod Config“ nicht gesetzt wurde.
4. Legen Sie für „Recv Auth“ den Wert „Either“ (oder „PAP“ oder „CHAP“) fest.
5. Verlassen Sie das Antwortprofil.

IPX-Bridging

Hinweis: Für IPX-Bridging gibt es spezielle Voraussetzungen, um NetWare-Client-Server-Logins über das WAN zu ermöglichen und zu verhindern, daß IPX-RIP- und -SAP-Broadcasts Bridging-Verbindungen unbegrenzt aufrechterhalten. Diese Voraussetzungen können mit den in Tabelle 6-2 aufgeführten Parametern geschaffen werden.

Tabelle 6-2: IPX-Bridging-Parameter

Ort	**Parameter mit Beispielwerten**
Ethernet > Connections > *alle Profile* > IPX options...	Handle IPX=Client *(für Client-Bridging)*
Ethernet > Connections > *alle Profile* > IPX options...	NetWare t/o=30 *(für Server-Bridging)* Handle IPX=Server

Wie alle Optionen im Untermenü „IPX Options“ ist der Parameter „Handle IPX“ nicht verfügbar („N/A“), wenn in „Ethernet-->Mod Config“ kein IPX-Rahmentyp (Parameter „IPX Frame“) angegeben ist. Wenn der Parameter „Route IPX“ im Verbindungsprofil den Wert „Yes“ hat, ist der Parameter „Handle IPX“ ebenfalls nicht verfügbar („N/A“), agiert aber so als hätte er den Wert „Server“.

- Bridging, wenn das lokale Netzwerk nur NetWare-Clients unterstützt

  Wenn das lokale Ethernet nur NetWare-Clients und keine NetWare-Server unterstützt, sollte die Bridging-Verbindung einen lokalen Client in die Lage versetzen, die WAN-Verbindung durch das Fragen nach einem NetWare-Server im entfernten Netzwerk aufzubauen. Damit die Verbindung jedoch nicht durch RIP- oder SAP-Broadcasts unbegrenzt aufrechterhalten wird, ist „Handle IPX=Client“ festzulegen.

- Bridging, wenn nur das lokale Netzwerk NetWare-Server unterstützt

  Wenn das lokale Netzwerk NetWare-Server (oder eine Kombination aus Clients und Servern) und das entfernte Netzwerk nur NetWare-Clients unterstützt, sollte die Pipeline durch die Bridging-Verbindung in die Lage versetzt werden, zwar auf NCP-Watchdog-Anforderungen für entfernte Clients zu reagieren, inaktive Verbindungen aber, wenn möglich, zu beenden. Dazu ist „NetWare t/o=30“ (Beispiel) und „Handle IPX=Server“ festzulegen.

- Bridging, wenn beide Seiten nur NetWare-Server unterstützen

  Wenn NetWare-Server auf beiden Seiten der WAN-Verbindung unterstützt werden, empfehlen wir dringend, statt einer IPX-Bridging-Verbindung eine IPX-Routing-Konfiguration zu verwenden. Bei IPX-Bridging-Verbindungen in einer solchen Umgebung gehen Client-Server-Logins verloren, sobald die Pipeline eine inaktive WAN-Verbindung beendet.

- IPX-Routing und Bridging auf ein und derselben Verbindung

  Wenn für eine Verbindung IPX-Routing aktiviert ist, kann die Pipeline nur einen einzigen Paket-Rahmentyp für IPX-Pakete über diese Verbindung „routen“. Wenn zum Beispiel als IPX-Rahmentyp (Parameter „IPX Frame“) „802.3“ festgelegt wurde, können nur 802.3-Pakete „geroutet“ werden. Verwenden einige der NetWare-Server im lokalen Netzwerk einen anderen Rahmentyp (z. B. „802.2“), werden diese Pakete „gebridgt“, falls Bridging aktiviert ist, bzw. ausgesondert, wenn Bridging nicht aktiviert ist.

  – Wenn im Verbindungsprofil „IPX Frame=802.3“ und „Route IPX=Yes“ und „Bridge=No“ festgelegt wurde, werden nur 802.3-IPX-Pakete „geroutet“; alle anderen Pakete werden ausgesondert.

  – Wenn im Verbindungsprofil „IPX Frame=802.3“ und „Route IPX=Yes“ und „Bridge=Yes“ festgelegt wurde, werden 802.3-IPX-Pakete „geroutet“ und alle anderen Pakete, wie IPX-Pakete mit anderen Rahmentypen, AppleTalk-Pakete, NetBios-Pakete usw., „gebridgt“.

Wenn die Pipeline zum Beispiel ein IPX-Paket mit einem 802.2-Rahmen empfängt, verwendet sie die physikalische Adresse in diesem Paket, um es über alle aktiven Bridging-Sitzungen zu „bridgen“.

Aktivieren von Bridging-Verbindungen

Die Pipeline verfügt über einen globalen Bridging-Parameter, der aktiviert sein muß, damit Bridging-Verbindungen funktionieren können. Der Parameter „Bridging“ führt dazu, daß der Ethernet-Controller der Pipeline-Einheit im promiskuitiven Modus („Promiscuous Mode“) läuft. Im promiskuitiven Modus akzeptiert der Ethernet-Treiber alle Pakete, unabhängig von deren Adresse oder Pakettyp, und leitet sie innerhalb der Protokollhierarchie nach oben weiter, damit in höheren Schichten festgelegt werden kann, ob das Paket zu „routen“, zu „bridgen“ oder zurückzuweisen ist.

Hinweis: Durch den promiskuitiven Modus entsteht ein größerer Prozessor- und Speicher-Overhead als beim Standardbetrieb des Ethernet-Controllers. Bei stark belasteten Netzwerken kann dieser größere Overhead zu einer Verlangsamung der Arbeitsgeschwindigkeit führen, selbst wenn keine Pakete „gebridgt“ werden.

Tabelle 6-3: Bridging-Parameter im Ethernet-Profil

Ort	Parameter mit Beispielwert
Ethernet > Mod Config (Ethernet-Profil)	Bridging=Yes

Zur Aktivierung des Bridging im Ethernet ist wie folgt vorzugehen:

1. Öffnen Sie „Ethernet-->Mod Config“.
2. Setzen Sie den globalen Bridging-Parameter („Bridging“) auf „Yes“.
   ```
   Bridging=Yes
   ```
3. Schließen Sie das Ethernet-Profil.

Verwalten der Bridging-Tabelle

Um „gebridgte“ Pakete zum richtigen Zielnetzwerk weiterleiten zu können, verwendet die Pipeline eine Bridging-Tabelle, in der für bestimmte Verbindungen bestimmte Endknoten festgelegt sind. Diese Tabelle, die dynamisch erstellt wird (siehe dazu „Transparentes Bridging“ auf Seite 6-10), enthält auch die Einträge in den Bridging-Profilen der Pipeline. Bridging-Profile fungieren analog zu statischen Routen in einer Routing-Umgebung. In Bridging-Profilen können bis zu 8 Zielknoten und die entsprechenden Verbindungsinformationen definiert werden.

Parameter mit Einfluß auf die Bridging-Tabelle

In Tabelle 6-4 finden Sie die Konfigurationsparameter, die direkten Einfluß auf die Bridging-Tabelle haben.

Tabelle 6-4: Parameter mit Einfluß auf die Bridging-Tabelle

Ort	Parameter mit Beispielwerten
Ethernet > Mod Config (Ethernet-Profil)	Bridging=Yes
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Bridge=Yes Dial Brdcast=No
Ethernet > Bridge Adrs > *alle Profile* (Bridging-Profil)	Enet Adrs=CFD012367 Net Adrs=10.1.1.12 Connection #=7
Ethernet > Answer > PPP options... (Antwortprofil)	Bridge=Yes

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Transparentes Bridging

Die Pipeline ist eine transparente („lernende“) Bridge. Sie „merkt“ sich, wo sich eine bestimmte Adresse befindet, und welches Verbindungsprofil für eine Verbindung zu dieser Adresse benötigt wird. Beim Weiterleiten von Paketen verwendet sie die Ausgangsadresse des jeweiligen Pakets zum Aufbau einer Bridging-Tabelle, die die Knotenadressen der Pakete mit einer bestimmten Schnittstelle verknüpfen.

So zeigt zum Beispiel Abbildung 6-2 die physikalische Adresse einiger Knoten im lokalen Ethernet und am entfernten Standort. Die Pipeline am Standort A ist als Bridge konfiguriert.

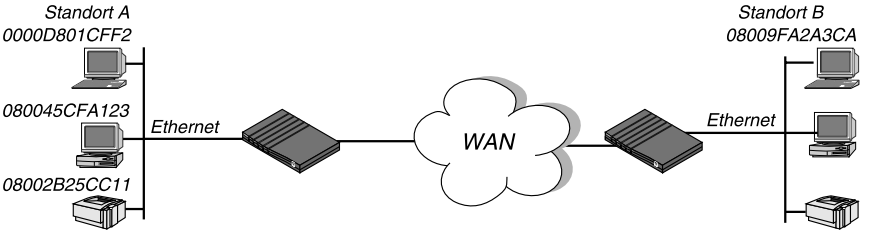


Abbildung 6-2: Erstellung einer Bridging-Tabelle durch die Pipeline

Die Pipeline am Standort A „lernt“ Schritt für Schritt die Adressen in beiden Netzwerken, indem sie die Ausgangsadressen der einzelnen Pakete prüft. Auf der Grundlage dieser Informationen erstellt sie dann eine Bridging-Tabelle, wie z. B. die folgende:

```
0000D801CFF2        SITEA
080045CFA123        SITEA
08002B25CC11        SITEA
08009FA2A3CA        SITEB (Connection Profile #5)
```

Das Verknüpfen eines Verbindungsprofils mit einer Bridging-Verbindung erfolgt, wenn das Profil zum Wählen der Verbindung verwendet wurde oder wenn es einem ankommenden Ruf entsprach.

Die Einträge in der Bridging-Tabelle müssen innerhalb eines festen Zeitraums erneut gelernt werden. Ist dies nicht der Fall, werden sie aus der Tabelle gelöscht.

Statische Bridging-Tabelleneinträge

Der Administrator kann bis zu 8 statische Bridging-Tabelleneinträge in Bridging-Profilen definieren. Bei Verbindungen, die über einen statischen Bridging-Tabelleneintrag verfügen, kann der Parameter „Dial Brdcast“ den Wert „No“ haben.

„Dial Brdcast“ ist eine sehr bequeme Möglichkeit, Pakete zu „bridgen“, wenn die Pipeline nur über einige wenige Bridging-Verbindungen verfügt. In einer Umgebung, in der viele Profile Bridging unterstützen, kann sich dies aber als kostspielig erweisen (siehe dazu „Broadcast-Adressen und der Parameter „Dial Brdcast““ auf Seite 6-4). Wenn „Dial Brdcast“ in einem Verbindungsprofil den Wert „No“ zugewiesen bekommen hat, wird diese Verbindung nicht durch Broadcast-Anforderungen gewählt. Statt dessen verläßt sich die Pipeline bei der Festlegung des zu verwendenden Verbindungsprofils auf ihre Bridging-Tabelle.

Hinweis: Wenn für den Parameter „Dial Brdcast“ der Wert „No“ festgelegt wird und die Pipeline keinen Bridging-Tabelleneintrag für eine Zieladresse findet, wird diese Verbindung nicht aufgebaut.

Zur Definition eines statischen Bridging-Tabelleneintrags ist wie folgt vorzugehen:

1 Öffnen Sie ein Bridging-Profil.

2 Geben Sie die physikalische Adresse des entfernten Hosts an.

Beispiel:

```
Enet Adrs=0080AD12CF9B
```

Nähere Informationen dazu finden Sie im Abschnitt „Physikalische Adressen und die Bridging-Tabelle“ auf Seite 6-3. Die Adresse erhalten Sie vom Administrator des entfernten Netzwerks.

3 Wenn es sich beim entfernten Ende um ein Segment des lokalen IP-Netzwerks handelt, ist eine Adresse in diesem Segment anzugeben.

Beispiel:

```
Net Adrs=10.2.3.133
```

Nähere Informationen dazu finden Sie im Abschnitt „Beispiel für eine IP Bridging-Verbindung“ auf Seite 6-20.

4 Geben Sie die Nummer des Verbindungsprofils für diese Verbindung an.
Beispiel:

```
Connection #=2
```

Sie müssen nicht die gesamte Nummer angeben. Der eindeutige Teil der Nummer reicht aus.

5 Schließen Sie das Bridging-Profil.

Konfigurieren von Bridging-Verbindungen

In diesem Abschnitt wird erläutert, wie Sie das Bridging für eine Pipeline konfigurieren können, die eine Verbindung mit einem entfernten Gerät aufbaut. Dieses Beispiel konzentriert sich ausschließlich auf das Bridging und beinhaltet daher weder die verbindungsspezifischen Einstellungen (wie die Optionen der jeweiligen Telefongesellschaft oder die MP+- bzw. Frame-Relay-Konfiguration) noch die zusätzlichen Routing-Einstellungen, die u. U. auf Ihrer Seite erforderlich sind.

In den Verbindungsprofilen muß Bridging aktiviert sein. Wenn das entfernte Netzwerk keinen statischen Bridging-Tabelleneintrag hat, muß außerdem „Dial Brdcast=Yes“ festgelegt werden.

Die Tabelle 6-4 enthält die Verbindungsprofil-Parameter, die Einfluß auf das protokollunabhängige Bridging haben.

Tabelle 6-5: Bridging-Parameter in Verbindungsprofilen

Ort	Parameter mit Beispielwerten
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Station=SITEBGW Bridge=Yes Dial Brdcast=No
Ethernet > Connections > *alle Profile* > Encaps options...	Send Auth=None Recv PW=N/A Send PW=N/A

Tabelle 6-5: Bridging-Parameter in Verbindungsprofilen (Fortsetzung)

Ort	Parameter mit Beispielwerten
Ethernet > Connections > *alle Profile* > IPX options...	Handle IPX=Client

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Beispiel für eine AppleTalk-Bridging-Verbindung

Für eine AppleTalk-Verbindung auf Verbindungsebene muß an beiden Enden der Verbindung eine Bridge vorhanden sein.

Die häufigste Fehlerursache bei der Ersteinrichtung von Bridging-Verbindungen ist die Angabe eines falschen Namens für die Pipeline oder des entfernten Geräts. Oftmals wird nicht auf die Groß- und Kleinschreibung geachtet, oder es werden Bindestriche, Leerzeichen oder Unterstriche vergessen. Stellen Sie also sicher, daß der Name genau so eingegeben wird, wie er im entfernten Gerät erscheint.

Bei diesem Beispiel wird davon ausgegangen, daß für den Parameter „Bridging“ in „Ethernet-->Mod Config“ der Wert „Yes“ festgelegt wurde (siehe dazu „Aktivieren von Bridging-Verbindungen“ auf Seite 6-8). Außerdem muß auch im Antwortprofil das Bridging aktiviert sein (siehe dazu „Bridging-Parameter im „Answer“-Profil“ auf Seite 6-5).

Hinweis: In diesem Beispiel ist für den Parameter „Dial Brdcast“ in den Verbindungsprofilen der Wert „No“ festgelegt worden, und es wurde ein Bridging-Profil definiert. Dies ist jedoch nicht unbedingt erforderlich. Sie können „Dial Brdcast“ aktivieren und das Bridging-Profil weglassen, wenn Sie dies wünschen.

Zum Konfigurieren der Pipeline am Standort A für eine Bridging-Verbindung ist wie folgt vorzugehen:

1 Öffnen Sie das Systemprofil.

2 Weisen Sie der Pipeline, falls noch nicht geschehen, einen Systemnamen zu.

Beispiel:

```
Name=SITEAGW
```

Bridging-Verbindungen verwenden Systemnamen für einen Teil des Authentifizierungsvorgangs.

3 Schließen Sie das Systemprofil.

4 Öffnen Sie das Verbindungsprofil #5.

5 Legen Sie die Werte für die folgenden Parameter fest:

```
Station=SITEBGW
Active=Yes
Encaps=PPP
Bridge=Yes
Dial Brdcast=No

Encaps options...
    Send Auth=CHAP
   Recv PW=*SECURE*
   Send PW=*SECURE*
```

6 Schließen Sie das „Connections“-Profil #5.

7 Öffnen Sie ein Bridging-Profil.

8 Legen Sie die Werte für die folgenden Parameter fest:

```
Enet Adrs=0080AD12CF9B
Net Adrs=0.0.0.0
Connection #=5
```

9 Schließen Sie das Bridging-Profil.

Zum Konfigurieren der Pipeline am Standort B für eine Bridging-Verbindung ist wie folgt vorzugehen:

1 Öffnen Sie das Systemprofil (der entfernten Pipeline).

2 Weisen Sie der Pipeline, falls noch nicht geschehen, einen Systemnamen zu.

Beispiel:

```
Name=SITEBGW
```

3 Schließen Sie das Systemprofil.

4 Öffnen Sie das „Connections“-Profil #2 der Pipeline.

5 Legen Sie die Werte für die folgenden Parameter fest:

```
Station=SITEAGW
Active=Yes
Encaps=PPP
Bridge=Yes
Dial Brdcast=No

Encaps option...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*
```

6 Schließen Sie das Verbindungsprofil #2.

7 Öffnen Sie ein Bridging-Profil.

8 Legen Sie die Werte für die folgenden Parameter fest:

```
Enet Adrs=0CFF1238FFFF
Net Adrs=0.0.0.0
Connection #=2
```

9 Schließen Sie das Bridging-Profil.

Beispiel für eine IPX-Client-Bridging-Verbindung (lokale Clients)

In diesem Beispiel unterstützt das lokale Ethernet NetWare-Clients, und das entfernte Netzwerk unterstützt sowohl NetWare-Server als auch NetWare-Clients.

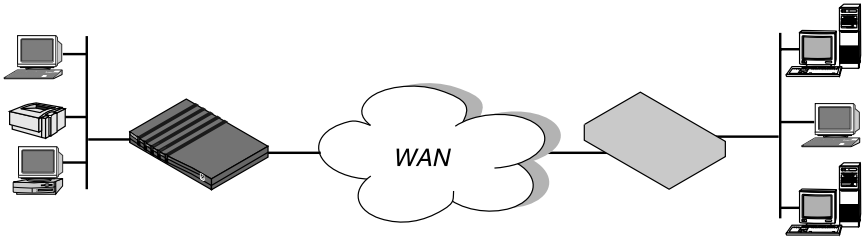


Abbildung 6-3: Beispiel für eine IPX-Client-Bridging-Verbindung

Zum Konfigurieren der Pipeline am Standort A in diesem Beispiel ist wie folgt vorzugehen:

1. Öffnen Sie das Systemprofil.
2. Weisen Sie der Pipeline, falls noch nicht geschehen, einen Systemnamen zu. Beispiel:

   ```
   Name=SITEAGW
   ```

3. Schließen Sie das Systemprofil.
4. Öffnen Sie „Ethernet-->Mod Config“.
5. Öffnen Sie das Untermenü „Ether Options“.
6. Legen Sie den Wert für den IPX-Rahmentyp fest (Parameter „IPX Frame“).

   ```
   IPX Frame=802.3
   ```

7 Schließen Sie „Ethernet-->Mod Config“.

8 Öffnen Sie ein „Connections“-Profil.

9 Legen Sie die Werte für die folgenden Parameter fest:

```
Station=SITEBGW
Active=Yes
Encaps=PPP
Route IPX=No
Bridge=Yes
Dial Brdcast=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    Handle IPX=Client
```

10 Schließen Sie das Verbindungsprofil.

„Dial Brdcast“ ist aktiviert, damit die Verbindung durch Dienstanforderungen aufgebaut werden kann.

Wenn „Handle IPX=Client“ festgelegt wird, weist die Pipeline einen Datenfilter zu, der periodische RIP- und SAP-Broadcasts an ihrer WAN-Schnittstelle aussondert, RIP- und SAP-Abfragen jedoch weiterleitet. Auf diese Weise können lokale Clients einen NetWare-Server über das WAN ausfindig machen, ohne daß die Verbindung unnötigerweise durch routinemäßige Broadcasts aufrechterhalten wird.

Beispiel für eine IPX-Server-Bridging-Verbindung (lokale Server)

In diesem Beispiel unterstützt das lokale Netzwerk eine Kombination aus NetWare-Clients und -Servern, und das entfernte Netzwerk unterstützt nur Clients.

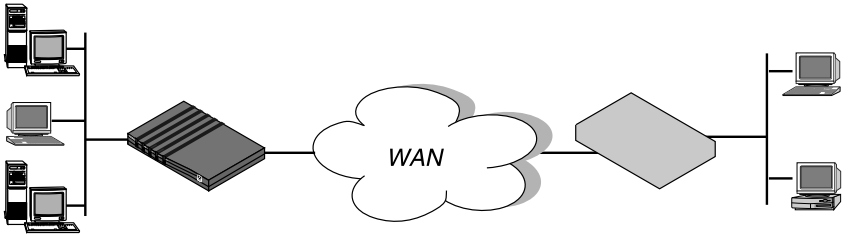


Abbildung 6-4: Beispiel für eine IPX-Server-Bridging-Verbindung

Zum Konfigurieren der Pipeline am Standort A in diesem Beispiel ist wie folgt vorzugehen:

1. Öffnen Sie das Systemprofil.
2. Weisen Sie der Pipeline, falls noch nicht geschehen, einen Systemnamen zu. Beispiel:

   ```
   Name=SITEAGW
   ```
3. Schließen Sie das Systemprofil.
4. Öffnen Sie „Ethernet-->Mod Config“.
5. Öffnen Sie das Untermenü „Ether Options“.
6. Legen Sie den Wert für den IPX-Rahmentyp fest (Parameter „IPX Frame“). Beispiel:

   ```
   IPX Frame=802.3
   ```

7 Schließen Sie „Ethernet-->Mod Config“.

8 Öffnen Sie ein „Connections“-Profil.

9 Legen Sie die Werte für die folgenden Parameter fest:

```
Station=SITEBGW
Active=Yes
Encaps=PPP
Route IPX=No
Bridge=Yes
Dial Brdcast=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    NetWare t/o=30
    Handle IPX=Server
```

10 Schließen Sie das „Connections“-Profil.

Wenn „Handle IPX=Server“ festgelegt wurde, weist die Pipeline einen Datenfilter zu, der RIP- und SAP-Broadcasts an ihrer WAN-Schnittstelle aussondert, aber RIP- und SAP-Abfragen weiterleitet. Außerdem nutzt die Pipeline den im Parameter „NetWare t/o“ festgelegten Wert als Zeitgrenze für die Antwort auf NCP-Watchdog-Anforderungen im Namen von Clients auf der anderen Seite der Verbindung (das sogenannte „Watchdog-Spoofing“).

Hinweis: Die Pipeline führt das Watchdog-Spoofing für den im Ethernet-Profil festgelegten IPX-Rahmentyp aus. Wenn z. B. für „IPX Frame“ der Wert „802.3“ festgelegt wurde, erfolgt das Spoofing nur bei Verbindungen zu Servern, die diesen Paketrahmentyp verwenden. Nähere Informationen zu diesem Thema finden Sie in Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“.

Beispiel für eine IP Bridging-Verbindung

Wenn Sie eine Bridging-Verbindung zwischen zwei Segmenten ein und desselben IP-Netzwerks herstellen wollen, können Sie den Parameter „Net Adrs“ in einem Bridging-Profil verwenden, um die Pipeline in die Lage zu versetzen, beim Aufbau der Bridging-Verbindung auf ARP-Anforderungen zu antworten.

Wenn ein ARP-Paket eine IP-Adresse enthält, die dem Wert des Parameters „Net Adrs“ in einem Bridging-Profil entspricht, antwortet die Pipeline auf die ARP-Anforderung mit der im Bridging-Profil angegebenen (physikalischen) Ethernet-Adresse und baut die angegebene Verbindung auf. Die Pipeline agiert also als ein Proxy für den Knoten mit dieser Adresse.

In diesem Beispiel sind zwei Segmente ein und desselben IP-Netzwerks über das WAN miteinander verbunden.

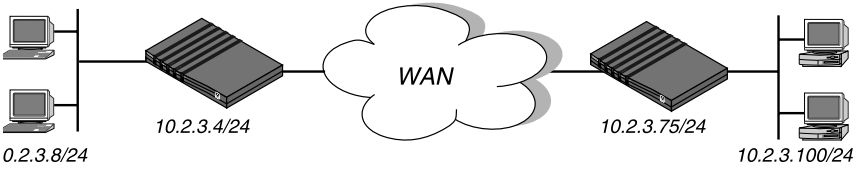


Abbildung 6-5: Beispiel für eine IP Bridging-Verbindung

Zum Konfigurieren der Pipeline am Standort A in diesem Beispiel ist wie folgt vorzugehen:

1 Öffnen Sie das Systemprofil.

2 Weisen Sie der Pipeline, falls noch nicht geschehen, einen Systemnamen zu. Beispiel:

```
Name=SITEAGW
```

3 Schließen Sie das Systemprofil.

4 Öffnen Sie das „Connections“-Profil #7 (zum Beispiel).

5 Legen Sie die Werte für die folgenden Parameter fest:

```
Station=SITEBGW
Active=Yes
Encaps=PPP
Route IP=No
Bridge=Yes
Dial Brdcast=No

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*
```

6 Schließen Sie das Verbindungsprofil #7.

7 Öffnen Sie ein Bridging-Profil.

8 Legen Sie die Werte für die folgenden Parameter fest:

```
Enet Adrs=0CFF1238FFFF
Net Adrs=10.2.3.100/24
Connection #=7
```

9 Schließen Sie das Bridging-Profil.

Konfigurieren der Pipeline als IP-Router

7

Dieses Kapitel enthält die folgenden Abschnitte:

Die Pipeline als IP-Router – Einführung

In dieser Einführung erfahren Sie, wie die Pipeline IP-Routing-Verbindungen aufbaut. Außerdem erhalten Sie einen Überblick über RIP-2, und es wird die Ascend-Netzmaskenkonvention beschrieben.

IP-Routing wird in der Pipeline vor allem zu den folgenden Zwecken eingesetzt:

- Aufbau von IP-Verbindungen zum Internet (über einen Internet-Service-Provider)
- Verbinden von verteilten IP-Subnetzen mit einem Unternehmensnetz (Telearbeit-Hubs)

Die Pipeline unterstützt IP-Routing über PPP-, MP-, MP+- und Frame-Relay-Verbindungen. Die Pipeline kann ohne Einschränkungen mit nicht von Ascend stammenden Produkten zusammenarbeiten, die ebenfalls TCP/IP unterstützen und den damit zusammenhängenden RFCs entsprechen.

IP-Routing-Verbindungen arbeiten mit einem bestimmten Maß an eingebauter Authentifizierung, da die Pipeline die IP-Adresse eines Verbindungsprofils mit der Ausgangs-IP-Adresse der rufenden Seite vergleicht. In den meisten Fällen reicht dieses Maß an Sicherheit jedoch nicht aus, so daß zusätzlich die PAP- bzw. CHAP-Authentifizierung zum Einsatz kommt. Siehe dazu Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Hinweis: IP-Routing kann zusammen mit dem protokollunabhängigen Bridging und dem IPX-Routing in jeder beliebigen Kombination konfiguriert werden. Es ist jedoch nicht möglich, TCP/IP-Pakete über ein und dieselbe Verbindung zu „bridgen“ und zu „routen“. Wenn Sie die Pipeline als einen IP-Router konfigurieren, findet kein Bridging in der Datensicherungsschicht („Data Link Layer“) mehr statt. Die Pakete werden *immer* in der Netzwerkschicht („Network Layer“) „geroutet“. Bei allen anderen Protokollen findet weiterhin Bridging statt, solange dies aktiviert bleibt. Nähere Informationen zum Bridging finden Sie in Kapitel 6, „Konfigurieren der Pipeline als Bridge“.

Verbindungen zwischen Host und Router

Wenn das Gerät, das eine Verbindung mit der Pipeline herstellt, ein Host ist, auf dem PPP-Einwählsoftware läuft, fügt die Pipeline ihrer Routing-Tabelle eine „Host-Route“ hinzu. Nähere Informationen zu Host-Routen finden Sie im Abschnitt „Die Ascend-Netzmaskenkonvention“ auf Seite 7-5.

Wenn der Host zu Ihrem eigenen IP-Netzwerk gehört, muß die Pipeline ein Verbindungsprofil haben, das die Adresse des Hosts enthält, wobei eine 32-Bit-ke zum Einsatz kommt.

Empfängt die Pipeline einen ankommenden Ruf, überprüft die Pipeline mit Hilfe ihres Antwortprofils, ob sie ankommende IP-Routing-Rufe akzeptieren kann. Dann wird überprüft, ob es ein Verbindungsprofil für die rufende Seite gibt. Wurde im Antwortprofil festgelegt, daß keine ankommenden IP-Routing-Rufe angenommen werden dürfen, oder gibt es kein Verbindungsprofil für den Ruf, wird der Ruf zurückgewiesen.

Wenn das Antwortprofil den ankommenden Ruf zuläßt, sucht die Pipeline nach einem Profil, das dem Benutzernamen und der IP-Adresse entspricht. Kann kein entsprechendes Profil gefunden werden, wird der Ruf beendet.

Hat die Pipeline eine Adresse gefunden und wurde diese von der PPP-Software akzeptiert, authentifiziert die Pipeline die Verbindung mit Hilfe von PAP bzw. CHAP und baut dann die Verbindung auf.

Nach dem Aufbau der Verbindung fügt die Pipeline ihrer Routing-Tabelle eine Host-Route hinzu und beginnt als IP-Router zwischen ihrer lokalen und der WAN-Schnittstelle zu agieren. Wurde die Pipeline für RIP konfiguriert, sendet sie außerdem ihre aktualisierte Routing-Tabelle an andere Hosts.

Verbindungen von Router zu Router

Wenn es sich bei dem Gerät, das eine Verbindung zur Pipeline herstellen will, um einen IP-Router in einem IP-Netzwerk handelt, ist die sich ergebende Verbindung eine Route zu diesem entfernten Netzwerk (bzw. Subnetz). So zeigt das Beispiel in Abbildung 7-1 eine mit einem entfernten Router verbundene Pipeline, wobei es sich bei den beiden Ethernet-Segmenten um zwei verschiedene IP-Netzwerke handelt.

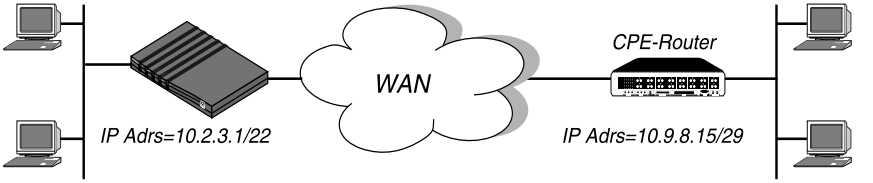


Abbildung 7-1: IP-Routing-Verbindung zwischen zwei Netzwerken

Wenn ein Benutzer am Standort B Telnet startet und eine Adresse an Standort A eingibt, empfängt der entfernte Router abgehende TCP/IP-Pakete, die er mit Hilfe seiner Routing-Tabelle überprüft. Findet er dort keine Route zum Standort A, leitet er, je nach Konfiguration, die Pakete entweder zu seinem Standard-Router weiter oder sondert sie aus. Wenn die Pipeline eine Route zum Standort A findet, öffnet sie das entsprechende Profil und wählt die Verbindung.

Beim Empfang eines Rufes überprüft die Pipeline ihr Antwortprofil und überprüft, ob sie ankommende IP-Routing-Rufe akzeptieren kann. Ist IP-Routing im Antwortprofil nicht aktiviert, beendet die Pipeline den Ruf.

Wurde IP-Routing im Antwortprofil aktiviert, sucht die Pipeline nach einem Profil, das der von der Pipeline bei der PPP-Verhandlung angebotenen IP-Adresse entspricht. Wenn die Pipeline kein entsprechendes Verbindungsprofil finden kann, beendet sie den Ruf.

Gibt es ein passendes Profil, authentifiziert die Pipeline die Verbindung mit Hilfe von PAP bzw. CHAP und baut dann die Verbindung auf.

Nach Aufbau der Verbindung fügt die Pipeline ihrer Routing-Tabelle eine Netzwerk-Route hinzu und beginnt, als IP-Router zwischen ihrer lokalen und der WAN-Schnittstelle zu agieren. Wurde die Pipeline für RIP konfiguriert, sendet sie außerdem ihre aktualisierte Routing-Tabelle an andere Hosts.

Wenn die Verbindung aufgebaut wurde, fügt die Pipeline ihrer Routing-Tabelle eine Route zum entfernten Netzwerk hinzu. Obgleich die zugewiesene Adresse sich im lokalen Netzwerk zu befinden scheint, arbeitet die Pipeline als Router zwischen ihrer lokalen und der WAN-Schnittstelle. Wurde die Pipeline für RIP konfiguriert, sendet sie ihre aktualisierte Routing-Tabelle an andere Hosts.

Die Ascend-Netzmaskenkonvention

In Ascend-Einheiten werden IP-Adressen im dezimalen Format (nicht im hexadezimalen Format) angegeben. Beispiel:

```
198.5.248.40
```

Wird keine Netzmaske angegeben, geht die Pipeline davon aus, daß eine Standard-Netzmaske auf der Grundlage der „Klasse“ der Adresse verwendet wird:

Tabelle 7-1: IP-Adressenklassen und Standard-Netzmasken

Klasse	Adreßbereich	Netzwerk-Bits
Klasse A	0.0.0.0 → 127.255.255.255	8
Klasse B	128.0.0.0 → 191.255.255.255	16
Klasse C	192.0.0.0 → 223.255.255.255	24
Klasse D	224.0.0.0 → 239.255.255.255	—
Klasse E (reserviert)	240.0.0.0 → 247.255.255.255	—

So hat beispielsweise eine Adresse der Klasse C, wie z. B. 198.5.248.40, 24 Netzwerk-Bits (siehe Abbildung 7-2). Damit bleiben 8 Bits für den Hostteil der Adresse übrig, so daß in Netzwerken der Klasse C maximal 255 Hosts unterstützt werden können.

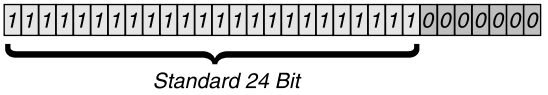


Abbildung 7-2: Adresse der Klasse C

Zur Festlegung einer Netzmaske verwenden Ascend-Einheiten nicht das dezimale Netzmaskenformat, wie z. B.:

```
IP Address=198.5.248.40
Netmask=255.255.255.248
```

Statt dessen wird ein Netzmasken-Modifikator verwendet, der die Gesamtzahl der Netzwerk-Bits in der Adresse angibt. Beispiel:

198.5.248.40/29

In der oben dargestellten Beispieladresse wird durch „/29“ angezeigt, daß zusätzliche 5 Bits der Adresse als eine Subnetznummer interpretiert werden.

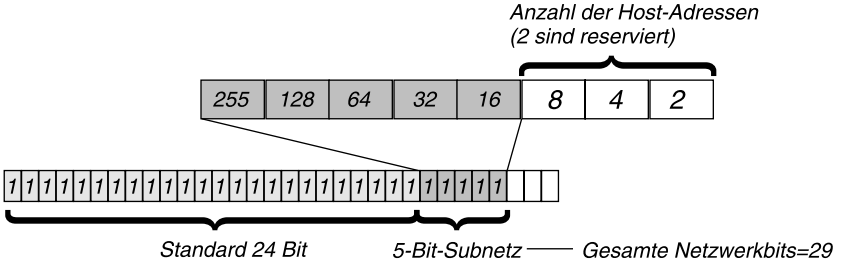


Abbildung 7-3: 29-Bit-Netzmaske und Anzahl der unterstützten Hosts

In 3 Bits sind acht Bitkombinationen möglich. Von diesen acht möglichen Hostadressen sind zwei reserviert:

000 – reserviert für die Netzwerkbasis (das Kabel)
001
010
100
110
101
011
111 – reserviert für die Broadcast-Adresse des Subnetzes

Tabelle 7-2 zeigt das Standard-Subnetz-Adreßformat im Vergleich mit der Ascend-Notation für Netzwerknummern der Klasse C.

Tabelle 7-2: Standard-Netzmaskenkonvention und Ascend-Netzmaskenkonvention

Netzmaske	Ascend-Notation	Anzahl der Hostadressen
255.255.255.0	/24	254 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.128	/25	126 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.192	/26	62 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.224	/27	30 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.240	/28	14 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.248	/29	6 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.252	/30	2 Hosts + 1 Broadcast, 1 Netzwerkbasis
255.255.255.254	/31	ungültige Netzmaske (keine Hosts)
255.255.255.255	/32	1 Host – eine Host-Route

Hinweis: Eine Host-Route ist eine spezielle IP-Adresse mit einer Subnetzmaske „/32“ (z. B. 198.5.248.40/32). Host-Routen werden für Einwählhosts benötigt.

Die Broadcast-Adresse von Subnetzen besteht immer nur aus Einsen. Die Netzwerkbasis-Adresse dient zur Angabe des Netzwerkkabels selbst. Dieses hat immer die Adresse 0. Wenn die Pipeline-Konfiguration einem entfernten Pipeline-Router z. B. die Adresse

```
198.5.248.120/29
```

zuweist, hat das mit diesem Router verbundene Ethernet den folgenden Adreßbereich:

```
198.5.248.120 – 198.5.248.127
```

Die Adresse „0“ (198.5.248.120) ist für das Kabel selbst reserviert. Die Broadcast-Adresse ist 198.5.248.127, und der Router selbst verwendet eine der Host-Adressen. Damit bleiben in diesem entfernten Subnetz fünf Hostadressen übrig, die in jeder beliebigen Reihenfolge auf fünf Hosts in diesem Subnetz verteilt werden können.

Anderes Beispiel: Wenn die Pipeline-Konfiguration einem entfernten Router die Adresse

```
192.168.8.64/26
```

zuweist, hat das mit diesem Router verbundene Ethernet den folgenden Adreßbereich:

```
192.168.8.64 – 192.168.8.127
```

Die „0“-Adresse für dieses Subnetz ist 192.168.8.64. Die Broadcast-Adresse muß die Netzwerkbasis-Adresse plus sechs Einsen sein (eigentlich 111111 zur Basis 2, also 63) – 192.168.8.127.

IP-Routing im Antwortprofil

Bevor die Pipeline einen ankommenden Ruf beantwortet, sucht sie im Antwortprofil nach Informationen, was zu tun ist. Enthält der Ruf nicht die vom Antwortprofil benötigten Informationen (wie Name und Kennwort), beendet die Pipeline den Ruf. Die folgenden Parameter im Antwortprofil wirken sich direkt auf das IP-Routing aus:

Tabelle 7-3: IP-Routing-Parameter im Antwortprofil

Ort	Parameter mit Beispielwerten
Ethernet > Answer (Antwortprofil)	Assign Adrs=Yes
Ethernet > Answer > Session options…	RIP=Off
Ethernet > Answer > PPP options...	Route IP=Yes Recv Auth=Either

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Hinweise dazu, was bei der Festlegung des Wertes für den Parameter „RIP“ im Antwortprofil zu beachten ist, können Sie dem Abschnitt „Konfigurieren von RIP für ankommende WAN-Verbindungen“ auf Seite 7-32 entnehmen.

Nähere Informationen zum Thema Authentifizierung finden Sie im Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Damit die Pipeline ankommende IP-Routing-Rufe beantwortet, sind die folgenden Schritte auszuführen:

1 Öffnen Sie das „Answer“-Profil.

2 Öffnen Sie das Untermenü „PPP Options“.

3 Aktivieren Sie das IP-Routing.

```
Route IP=Yes
```

4 Legen Sie für „Recv Auth“ den Wert „Either“, „PAP“ oder „CHAP“ fest.

Verbindungsprofile und IP-Routen

Die Pipeline legt beim Hochfahren eine Routing-Tabelle an und fügt der Tabelle alle Routen zu, die ihr bekannt sind, einschließlich der verbundenen Routen (z. B. Ethernet) und der Routen, die in ihren eigenen Verbindungsprofilen und „Static Rtes“-Profilen zu finden sind. Wenn im Ethernet RIP aktiviert ist, werden auch die Routen hinzugefügt, die sie von anderen Routern „gelernt“ hat. Ist RIP für eine aktive Verbindung aktiviert, werden zusätzlich die Routen in die Tabelle aufgenommen, die von der anderen Seite dieser Verbindung empfangen wurden.

Es gibt einige statische Routen, die die Pipeline beim Hochfahren nicht lesen kann. Diese Routen werden erst in die Routing-Tabelle aufgenommen, wenn sie funktionieren und verwendbar sind. Dazu gehören Routen, die über den Terminal-Server-Befehl „IPROUTE ADD“ hinzugefügt wurden.

Verwendung der Routing-Tabelle durch die Pipeline

Wenn die Pipeline ein IP-Paket im Ethernet empfängt, dessen Ziel sich nicht in diesem Netzwerk befindet, sucht sie in ihrer Routing-Tabelle nach einem Eintrag für das Zielnetzwerk:

- Findet die Pipeline eine Route zu diesem Netzwerk, leitet sie das Paket an den durch diese Route angegebenen Netzkoppler weiter. Ist dieser nicht lokal, öffnet sie eine WAN-Verbindung für die Weiterleitung des Pakets.
- Findet die Pipeline keine Route zu diesem Netzwerk, werden die Pakete an den Standard-Router weitergeleitet.
- Findet die Pipeline keine Route zu diesem Netzwerk und wurde keine Standard-Route konfiguriert, wird das Paket ausgesondert.

Wenn die Pipeline einen ankommenden IP-Routing-Ruf empfängt, überprüft sie die Ausgangs-IP-Adresse und sucht nach einem passenden Profil:

- Gibt es ein passendes Verbindungsprofil in der Pipeline, nimmt sie die Route zurück zum Ausgangsnetzwerk in die Routing-Tabelle auf, falls diese dort nicht bereits eingetragen ist.

Tritt der unwahrscheinliche Fall ein, daß das Antwortprofil ohne Authentifizierungsmaßnahmen konfiguriert ist und für den Parameter „Profile Reqd“ der Wert „No“ festgelegt wurde, akzeptiert die Pipeline alle ankommenden IP-Routing-Verbindungen. In diesem Fall gibt es keine Route für die ankommende Ausgangs-IP-Adresse, so daß unter Zuhilfenahme einer angenommenen Klasse-A- (8)-, -B-(16)- oder -C-(24)-Netzmaske für die Ausgangs-IP-Adresse eine temporäre Route erstellt wird. Wenn es sich dabei um eine Verbindung mit einem nicht von Ascend stammenden Router oder einen Host handelt, der die temporäre Anfangsroute nicht erkennt, muß u. U. entweder RIP aktiviert oder eine statische Route angelegt werden, um eine Route zu diesem Netzwerk zu erhalten.

RIP-2-Routing und RIP-1-Routing

In der Pipeline ist die Version 2 des RIP (Routing Information Protocol) implementiert, die eine Reihe von Verbesserungen gegenüber RIP-1 beinhaltet. Sie können die Pipeline so konfigurieren, daß sie RIP-1 oder RIP-2 an der Ethernet- oder jeder WAN-Schnittstelle entweder nur sendet, nur empfängt oder sendet und empfängt.

Hinweis: RIP-2 ist ein kompatibles Upgrade von RIP-1. Ascend empfiehlt jedoch, RIP-2 und RIP-1 nicht so in ein und demselben Netzwerk zu verwenden, daß die Router die Bekanntmachungen der anderen Router empfangen können. RIP-1 „erät“ Subnetzmasken, während RIP-2 diese nur explizit bearbeitet. Werden beide Versionen gemeinsam in einem Netzwerk verwendet, kann es passieren, daß RIP-1-„Ratereien“ zutreffende Subnetz-Informationen, die über RIP-2 bezogen wurden, außer Kraft setzen.

RIP-2 enthält gegenüber RIP-1 die folgenden Verbesserungen:

- Subnetz-Routing

  Der größte Unterschied zwischen RIP-1 und RIP-2 besteht darin, daß RIP-2-Routen Subnetzmasken-Informationen enthalten.

  RIP-1 konnte Subnetz-Informationen nur innerhalb des Subnetzes erkennen, und hat mit Absicht keine Netzmasken zu anderen Routern bekanntgemacht. Es gab, mit Ausnahme von direkt mit dem Subnetz verbundenen Routern, keine Möglichkeit, zwischen einem Subnetz- und einem Hosteintrag zu unterscheiden. Wenn ein RIP-1-Router eine IP-Adresse empfängt, verwendet er die Standard-Subnetzmaske.

RIP-2 leitet die Netzmaske zusammen mit der Adresse weiter. Dies macht nicht nur ein zuverlässiges Subnetz-Routing möglich, sondern läßt auch die Verwendung von Masken mit variabler Länge innerhalb ein und desselben Netzwerks sowie CIDR (Class-less Inter-Domain Routing) zu.

Wenn ein RIP-1-Router eine RIP-2-Aktualisierung empfängt, die Netzmasken beinhaltet, ignoriert er die Subnetz-Informationen.

- Authentifizierung

  RIP-1 enthielt keine Möglichkeit, seine Routing-Bekanntmachungen zu authentifizieren. Jedes Programm, daß Pakete über den UDP-Port 520 sendete, wurde als Router mit gültigen Distanzvektoren angesehen.

  RIP-2-Pakete verfügen über ein Authentifizierungsfeld, das ein einfaches Kennwort enthalten kann.

  Wenn ein RIP-1-Router ein RIP-2-Paket empfängt, das ein Kennwort enthält, wird dieses Feld ignoriert.

- Routing-Domänen

  Damit mehrere Netzwerke einen gemeinsamen Backbone nutzen können, verwendet RIP-2 eine Routing-Domänennummer, die es Routern erlaubt zu unterscheiden, für welches der Netzwerke des Routers das jeweilige Paket bestimmt ist.

- Multicasting

  RIP-1 verwendet eine Broadcast-Adresse für das Senden von Aktualisierungen. Das heißt, daß die Tabellen nicht nur von den Routern empfangen werden, sondern auch von allen Hosts am Kabel.

  RIP-2 verwendet eine IP-Multicast-Adresse für periodische Multicasts, die ausschließlich an RIP-2-Router gesendet werden. Dies ist ein Bereich, bei dem es möglicherweise zu Inkompatibilitäten mit RIP-1 kommen kann, da RIP-1-Knoten u. U. nicht die Multicasts empfangen können. Die Pipeline kann jedoch so konfiguriert werden, daß sie speziell mit RIP-1 interagiert. Dies wird allerdings nicht empfohlen.

Integrieren der Pipeline in das lokale IP-Netzwerk

Um die Pipeline mit Ihrem lokalen IP-Netzwerk zu verbinden, müssen Sie der Pipeline-Ethernet-Schnittstelle eine IP-Adresse zuweisen. Außerdem empfiehlt es sich u. U., eine oder mehrere der folgenden Aufgaben auszuführen:

- Aktivieren des Proxy-ARP, damit die Pipeline auf ARP-Anforderungen für entfernte Knoten reagieren kann
- Konfigurieren von DNS- bzw. WINS-Informationen, damit ankommende Telnet-Sitzungen mit Hilfe von Hostnamen möglich sind
- Konfigurieren der Pipeline, damit diese UDP-Prüfsummen generiert
- Aktualisieren anderer IP-Router im Netz

Tabelle 7-4 zeigt die relevanten Konfigurationsparameter.

Tabelle 7-4: IP-Routing-Parameter im Ethernet-Profil

Ort	**Parameter mit Beispielwerten**
Ethernet > Mod Config> Ether options… (Ethernet-Profil)	IP Adrs=10.2.3.1/24 2nd Adrs=10.128.8.55/24 Proxy-Modus=Off UDP Cksum=Yes
Ethernet > Mod Config > DNS…	Domain Name=abc.com Pri DNS=10.2.3.56/24 Sec DNS=10.2.3.107/24 List Attempt=No
Ethernet > Static Rtes > *alle Profile* („Static Rtes“-Profil)	Name=xyz.com Active=Yes Dest=198.2.3.0/24 Gateway=198.2.3.4 Metric=2 Preference=100 Private=No

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch.*

Nähere Informationen zur Verwendung von RIP im Ethernet finden Sie im Abschnitt „Aktivieren des dynamischen Routings für die Pipeline“ auf Seite 7-30.

Zuweisen der IP-Adresse für die Ethernet-Schnittstelle

Die Ethernet-Schnittstelle der Pipeline muß eine eigene, eindeutige IP-Adresse haben, die mit den Adressen anderer Hosts und Router im selben Netzwerk konsistent ist.

Zum Zuweisen einer IP-Adresse zur Ethernet-Schnittstelle der Pipeline ist wie folgt vorzugehen:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Öffnen Sie das Untermenü „Ether Options“.

3 Geben Sie im Parameter „IP Adrs“ die IP-Adresse für die Ethernet-Schnittstelle der Pipeline an.

Beispiel:

```
IP Adrs=10.2.3.1
```

4 Schließen Sie das Ethernet-Profil.

Nachdem Sie die IP-Adresse konfiguriert haben, können Sie von einem Host aus mit Hilfe des Befehls „PING“ überprüfen, ob die Pipeline ordnungsgemäß in das Netzwerk eingebunden ist. Siehe dazu „Überprüfen der Adresse mit Hilfe des Befehls „PING““ auf Seite 7-18.

Aufbau eines Subnetzes für die Pipeline

In großen Unternehmensnetzen werden an vielen Standorten Subnetze konfiguriert, um mehr Adressen für das Netzwerk zur Verfügung zu haben, komplexe Netzwerke zu segmentieren und das Routing in der lokalen Umgebung zu steuern. Stellen Sie sich zum Beispiel vor, das Haupt-Backbone-IP-Netzwerk ist 10.0.0.0 und unterstützt einen Backbone-Router mit der Adresse 10.0.0.17.

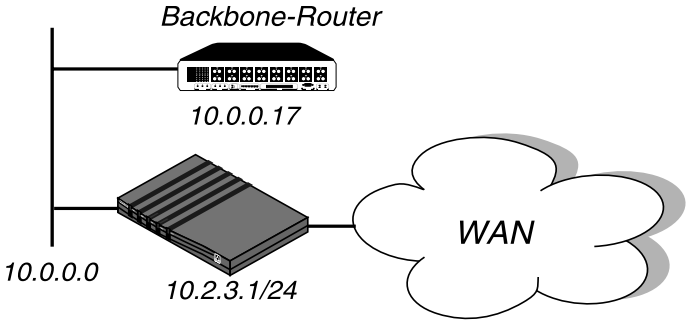


Abbildung 7-4: Aufbau eines Subnetzes für die Pipeline

Sie können die Pipeline in einem Subnetz dieses Netzwerks plazieren, indem Sie die IP-Adresse um eine Subnetzmaske erweitern. Gehen Sie dazu wie folgt vor:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Öffnen Sie das Untermenü „Ether Options“.

3 Geben Sie im Parameter „IP Adrs“ die IP-Adresse für die Ethernet-Schnittstelle der Pipeline an.

Beispiel:

```
IP Adrs=10.2.3.1/24
```

4 Schließen Sie das Ethernet-Profil.

Mit dieser Subnetz-Adresse benötigt die Pipeline eine statische Route zum Backbone-Router im Hauptnetz, da sie sonst nur die Subnetze „sehen“ kann, mit denen sie direkt verbunden ist.

Zum Erstellen der statischen Route und Einrichten des Backbone-Routers als Standardroute ist wie folgt vorzugehen:

1 Öffnen Sie das Menü „Static Rtes“.

2 Öffnen Sie das Profil „Default“.

3 Geben Sie im Parameter „Gateway“ die IP-Adresse eines Backbone-Routers an.

Beispiel:

```
Gateway=10.0.0.17
```

4 Lassen Sie die Standardwerte für die anderen Parameter unverändert. Beispiel:

```
Active=Yes
Dest=0.0.0.0/0
Metric=1
Private=Yes
```

5 Schließen Sie das „Static Rtes“-Profil „Default“.

Zuweisen von zwei Adressen: „Dual IP“

Die Pipeline kann einem einzelnen physikalischen Ethernet-Anschluß und der Route zwischen Pipeline und Anschluß zwei getrennte IP-Adressen zuweisen. Diese Funktion, die häufig als „Dual IP“ bezeichnet wird, gibt der Pipeline eine logische Schnittstelle in zwei Netzwerken oder Subnetzen über ein und denselben Backbone.

Im Normalfall gehören Geräte, die an dasselbe physikalische Kabel angeschlossen sind, alle zu ein und demselben IP-Netzwerk. Bei „Dual IP“ kann ein einzelnes Kabel zwei separate IP-Netzwerke unterstützen, wobei die Geräte am Kabel unterschiedlichen Netzwerken zugewiesen sind. Die Kommunikation erfolgt per Routing durch die Pipeline.

„Dual IP“ wird auch zur Verteilung der Routing-Verkehrslast auf ein großes Subnetz verwendet, indem IP-Adressen in diesem Subnetz zwei oder mehreren Routern am Backbone zugewiesen werden. Wenn die Router eine direkte Verbindung zum Subnetz und zum Backbone-Netzwerk aufgebaut haben, „routen“ sie Pakete zu diesem Subnetz und nehmen die Route in ihre Aktualisierungen der Routing-Tabelle auf.

„Dual IP“ ermöglicht Ihnen darüber hinaus einen sanften Übergang bei der Änderung von IP-Adressen. Dabei kann eine zweite IP-Adresse als eine Art Platzhalter agieren, während Sie die IP-Adressen in anderen Netzwerkgeräten ändern.

Abbildung 7-6 zeigt zwei Router, die mit einer zweiten Adresse in ein und demselben Subnetz konfiguriert sind.

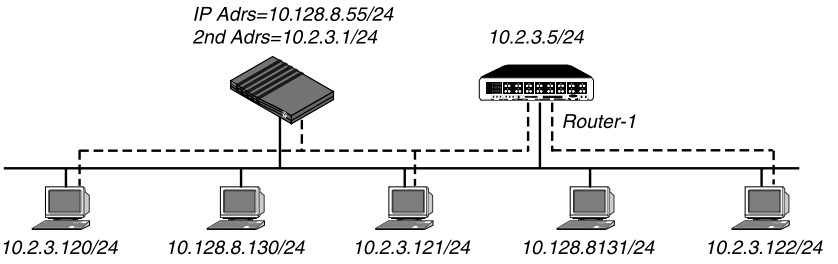


Abbildung 7-5: „Dual IP“ und gemeinsames Subnetz-Routing

Hinweis: Die zweite IP-Adresse wird zuweilen auch als Platzhalteradresse verwendet, während das lokale IP-Netzwerk auf eine andere Netzwerkadresse umgeschaltet wird.

Zum Zuweisen zweier Adressen zur Ethernet-Schnittstelle der Pipeline ist wie folgt vorzugehen:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Öffnen Sie das Untermenü „Ether Options“.

3 Geben Sie im Parameter „IP Adrs“ die IP-Adresse für die Ethernet-Schnittstelle der Pipeline an.

Beispiel:

```
IP Adrs=10.2.3.1/24
```

4 Geben Sie im Parameter „2nd Adrs“ die zweite IP-Adresse an.

Beispiel:

```
IP Adrs=10.128.8.55/24
```

Nach der Konfiguration der IP-Adressen können Sie von einem anderen IP-Host in jedem der IP-Subnetze aus mit Hilfe des Befehls „PING“ überprüfen, ob auf beide logischen Schnittstellen zugegriffen werden kann.

Hinweis: Damit andere Router die Pipeline in einem der beiden Netzwerke erkennen können, muß entweder im Ethernet-Profil RIP aktiviert werden, oder es müssen statische Routen in diesen Routern konfiguriert werden.

5 Schließen Sie das Ethernet-Profil.

Überprüfen der Adresse mit Hilfe des Befehls „PING“

Der Befehl „PING“ sendet ein ICMP-Datagramm mit obligatorischer Echoanforderung, das bei der entfernten Station anfragt: „Bist du da?“ Wenn die entfernte Station die Echoanforderung empfängt, sendet sie ein ICMP-Echoantwort-Datagramm zurück, in dem dem Sender mitgeteilt wird „Ja, ich bin da und bereit.“ Durch diesen Nachrichtenaustausch wird überprüft, ob der Übertragungsweg zwischen der Pipeline und der anderen Station offen ist.

Zur Überprüfung, daß die Pipeline im lokalen Netzwerk einsatzbereit ist, müssen Sie den Terminal-Server aufrufen und den folgenden Befehl eingeben:

```
ping <Hostname>
```

Beispiel:

```
ping 10.1.2.3
```

Sie können den PING-Nachrichtenaustausch mit Hilfe der Tastenkombination Strg-C jederzeit abbrechen. Weitere Informationen zur Verwendung des Befehls „PING“ erhalten Sie im Kapitel 11, „Systemadministration“.

Aktivieren des Proxy-Modus in der Pipeline

Wenn ein Einwählhost eine IP-Adresse im selben Netzwerk wie die Pipeline hat, „weiß“ nur die Pipeline, daß Pakete, die an diesen Host adressiert sind, über das WAN „geroutet“ werden müssen. Für andere lokale Router und Hosts scheint sich die Adresse im lokalen Netzwerk zu befinden. Sie können den Proxy-Modus in der Pipeline aktivieren, um sie in die Lage zu versetzen, auf ARP-Anforderungen (Adresse Resolution Protocol) für diese „lokalen“ Adressen zu reagieren, die nur über das WAN zu erreichen sind.

ARP ist ein Broadcast-Protokoll, das die physikalische Adresse eines Hosts findet, wenn dessen IP-Adresse bekannt ist. Wenn z. B. ein Benutzer eine FTP-Verbindung zu einem anderen IP-Host mit Hilfe dessen Namens aufbaut, bezieht die Host-Software die IP-Adresse für diesen Hostnamen über das DNS und fordert die TCP/IP-Software auf, eine Verbindung zu dieser Adresse aufzubauen. Befindet sich die IP-Adresse im lokalen IP-Netzwerk, sendet die Host-Software ARP-Anforderungen an alle Hosts im Ethernet, in denen diese aufgefordert werden, mit ihrer IP-Adresse zu antworten, wenn diese IP-Adresse ihnen gehört. IP-Pakete werden dann direkt an den antwortenden Host gesendet.

Befindet sich die IP-Adresse *nicht* im lokalen Netzwerk, wird keine ARP-Anforderung gesendet. Die Host-Software ist häufig so konfiguriert, daß die IP-Adresse der Pipeline als Standard-Router agiert und Pakete, die für entfernte Netzwerke bestimmt sind, stets an den Standard-Router weitergeleitet werden.

Bei Verbindungen zwischen Host und Netzwerk, bei denen einem entfernten Host eine IP-Adresse im lokalen Netzwerk zugewiesen ist, betrachtet die lokale TCP/IP-Software die IP-Adresse jedoch als lokal und sendet ARP-Anforderungen. In diesen Fällen kann die Pipeline den Proxy-Modus verwenden, um bei nicht-lokalen IP-Adressen mit ihrer eigenen MAC-Adresse zu antworten.

Um die Pipeline in die Lage zu versetzen, auf ARP-Anforderungen für entfernte Geräte zu reagieren, die lokale IP-Adressen haben, ist wie folgt vorzugehen:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Öffnen Sie das Untermenü „Ether Options“.

3 Aktivieren Sie den Proxy-Modus.

Wenn die IP-Adressen dynamisch zugewiesen wurden, ist folgende Einstellung zu verwenden:

```
Proxy Mode=Active
```

Wurden die IP-Adressen statisch zugewiesen, muß folgendes festgelegt werden:

```
Proxy Mode=Always
```

4 Schließen Sie das Ethernet-Profil.

Aktivieren von DNS

Wenn das lokale Netzwerk DNS-Server (Domain Name System) unterstützt, können Sie im Ethernet-Profil den Namen der lokalen Domäne und die IP-Adressen dieser Server festlegen.

„Weiß“ die Pipeline von DNS, können bei der Eingabe von TCP/IP-Befehlen, wie „TELNET“ und „PING“, über die Terminal-Server-Schnittstelle der Pipeline Hostnamen statt IP-Adressen verwendet werden. Außerdem hilft der Parameter „List Attempt“, das Abbrechen physikalischer Verbindungen zu verhindern, indem er den Benutzer in die Lage versetzt, die Einträge in der DNS-Liste der Hostnamen der Reihe nach zu versuchen, bis eine Verbindung zustandekommt.

Um die Pipeline über DNS in Kenntnis zu setzen, ist wie folgt vorzugehen:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Öffnen Sie das Untermenü „DNS“.

3 Geben Sie Ihren Domänennamen ein.

Beispiel:

```
Domain Name=eng.abc.com
```

4 Geben Sie die IP-Adresse des primären und des sekundären DNS-Servers ein.

Beispiel:

```
Pri DNS=10.2.3.56
```

```
Sec DNS=10.2.3.107
```

5 Aktivieren Sie den Parameter „List Attempt“, wenn es bei Ihnen möglich ist, mehrere Adressen für einen DNS-Hostnamen zu verwenden.

```
List Attempt=Yes
```

Dadurch wird der Benutzer in die Lage versetzt, die Einträge in der DNS-Liste der Hostnamen der Reihe nach zu versuchen, bis eine Verbindung zustandekommt.

6 Schließen Sie das Ethernet-Profil.

Generieren von UDP-Prüfsummen

UDP unterstützt die optionale Verwendung eines Prüfsummenfeldes zur Überprüfung der Integrität des UDP-Headers und der Daten. Die Pipeline überprüft bei jedem UDP-Paket, das sie empfängt, das UDP-Prüfsummenfeld und generiert Ethernet- und PPP-Prüfsummen für die entsprechenden Pakete. Es werden aber keine UDP-Prüfsummen generiert, solange der Parameter „UDP Cksum“ nicht aktiviert ist.

UDP-Prüfsummen sollten immer dann verwendet werden, wenn die Datenintegrität von besonders großer Wichtigkeit für Ihre Umgebung ist und redundante Überprüfungen benötigt werden. UDP-Prüfsummen sind auch angebracht, wenn sich Ihre UDP-Server am entfernten Ende einer WAN-Verbindung befinden, die anfällig für Fehler ist.

Die Pipeline verwendet UDP für die Generierung von Anfragen und Antworten für die folgenden Protokolle:

- SYSLOG
- DNS
- ECHOSERV
- RIP
- SNTP
- TFTP

Um die Pipeline so zu konfigurieren, daß Prüfsummen für diese Pakete generiert werden sollen, ist wie folgt vorzugehen:

1 Öffnen Sie das Ethernet-Profil.

2 Aktivieren Sie den Parameter „UDP Cksum“.

```
UDP Cksum=Yes
```

3 Schließen Sie das Ethernet-Profil.

Aktualisieren anderer Router am Backbone

Wenn die Routing-Tabellen anderer lokaler Router aktualisiert werden sollen, sobald die Pipeline eine Verbindung zu einem entfernten Gerät aufbaut, ist die Pipeline so zu konfigurieren, daß sie RIP-Aktualisierung über die Ethernet-Schnittstelle sendet. Die Pipeline sendet dann RIP-Pakete mit Informationen zu den einzelnen Routenänderungen. RIP-Aktualisierungen werden alle 30 Sekunden gesendet, so daß innerhalb ca. einer Minute alle Router im lokalen Netzwerk über die neue Route informiert sind. Sie können die Pipeline auch so konfigurieren, daß sie RIP-Aktualisierungen über das Ethernet nur empfängt oder sowohl sendet als auch empfängt. Siehe dazu „Konfigurieren von RIP im Ethernet-Profil“ auf Seite 7-31.

Verwalten der Routing-Tabelle

Die Routing-Tabelle der Pipeline wird erstellt, sobald die Pipeline hochgefahren wird (siehe dazu „Verbindungsprofile und IP-Routen“ auf Seite 7-10). Zur Verwaltung der Routing-Tabelle können Sie eine oder mehrere der folgenden Aufgaben ausführen:

- Konfigurieren statischer Routen in IP-Routing- und „Connections“-Profilen
- Konfigurieren einer Standardroute für Pakete mit unbekanntem Ziel
- Deaktivieren von „ICMP-Redirects“
- Konfigurieren von RIP-1 bzw. RIP-2 im Ethernet
- Deaktivieren von RIP bei WAN-Verbindungen
- Zuweisen der Präferenz für RIP oder statische Routen („Routenpräferenzen“)
- Anzeigen der Routing-Tabelle

Routing-Tabellen-Parameter

In Tabelle 7-5 werden die Parameter aufgeführt, die mit der IP-Routing-Tabelle der Tabelle in Zusammenhang stehen.

Tabelle 7-5: IP-Routing-Tabellen-Parameter

Ort	**Parameter mit Beispielwerten**
Ethernet > Mod Config (Ethernet-Profil)	RIP Policy=Poison Rvrs *(nur RIP-1)* RIP Summary=Yes *(nur RIP-1)* ICMP Redirects=Accept Adv Dialout Routes=Trunks Up
Ethernet > Mod Config > Ether options…	IP Adrs=10.2.3.2/245 2nd Adrs=0.0.0.0/0 RIP=Both-v2 Ignore Def Rt=No
Ethernet > Connections > *alle Profile* > (Verbindungsprofil)	Route IP=Yes
Ethernet > Connections > *alle Profile* > IP options…	LAN Adrs=10.9.8.10/22 WAN Alias=0.0.0.0 Metric=1 Preference=100 Private=No RIP=Off
Ethernet > Static Rtes > *alle Profile* („Static Rtes“-Profil)	Name=StandortBGW Active=Yes Dest=10.2.3.0/24 Gateway=10.2.3.4 Metric=2 Preference=100 Private=No
Ethernet > Answer (Antwortprofil)	Assign Adrs=Yes

Tabelle 7-5: IP-Routing-Tabellen-Parameter

Ort	Parameter mit Beispielwerten
Ethernet > Answer > PPP options…	Route IP=Yes
Ethernet > Answer > Session options…	RIP=Both-v2

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Hinweis: Gibt es in ein und demselben Netzwerk mehrere, redundant konfigurierte Pipelines, können Sie die Pipeline mit Hilfe des Parameters „Adv Dialout Routes“ anweisen, das Bekanntmachen von IP-Routen, die Wähldienste verwenden, zu stoppen, wenn sich ihre Leitungen aus irgendeinem Grund im Alarmzustand befinden. Wenn eine der redundanten Pipeline-Einheiten seine Wählleitungen vorübergehend verliert und für den Parameter „Adv Dialout Routes“ der Wert „Always“ angezeigt wird, empfängt die Einheit weiterhin abgehende Pakete, die zur redundanten Pipeline weitergeleitet werden sollen. Um dieses Problem bei der Verwendung von redundanten Einheiten zu verhindern, sollte der Parameter „Adv Dialout Routes“ auf „Trunks Up“ gesetzt werden. Näheres dazu können Sie dem *Referenzhandbuch* entnehmen.

Statische und dynamische Routen

Eine statische Route ist ein Pfad von einem Netzwerk zu einem anderen, in dem das Zielnetzwerk und der Router für den Weg dorthin angegeben ist. Bei Routen, bei denen es auf Zuverlässigkeit ankommt, werden vom Administrator häufig mehrere Pfade (sekundäre Routen) konfiguriert. In diesen Fällen wählt die Pipeline die primäre Route auf der Grundlage einer zugewiesenen Metrik.

Eine dynamische Route ist ein Pfad zu einem anderen Netzwerk, der dynamisch „erlernt“ wurde, statt in einem Profil konfiguriert zu werden. Router, die mit RIP arbeiten, versenden alle 30 Sekunden ihre gesamte Routing-Tabelle als Broadcast und informieren auf diese Weise andere Router darüber, welche Routen verwendet werden können. Hosts, auf denen ICMP läuft, können auch ICMP-Redirects senden, um einen besseren Pfad zu einem Zielnetzwerk anzubieten.

Hinweis: Dynamische Routen können statische Routen zum selben Netzwerk überschreiben oder „verbergen“, wenn die Metrik der dynamischen Route niedriger ist als die der statischen Route. Da dynamische Routen aber veralten („Aging“) und letztendlich ungültig werden, wenn keine entsprechenden Aktualisierungen vorgenommen werden, können „verborgene“ statische Routen nach einiger Zeit wieder in der Routing-Tabelle auftauchen.

Konfigurieren von statischen Routen

Jedes Verbindungsprofil, in dem eine explizite IP-Adresse angegeben ist, ist eine statische Route. Nähere Informationen zum Konfigurieren von Verbindungen finden Sie im Abschnitt „Konfigurieren von IP-Routing-Verbindungen“ auf Seite 7-39.

Das Netzwerkdiagramm in Abbildung 7-6 zeigt eine statische Route zu dem im Parameter „LAN Adrs“ angegebenen Subnetz (10.9.8.10/22) eines Verbindungsprofils. Mit diesem Parameter „LAN Adrs“ ist die implizierte statische Route mit diesen Adressen definiert:

- Dest=10.9.8.10/22
- Gateway=10.9.8.10

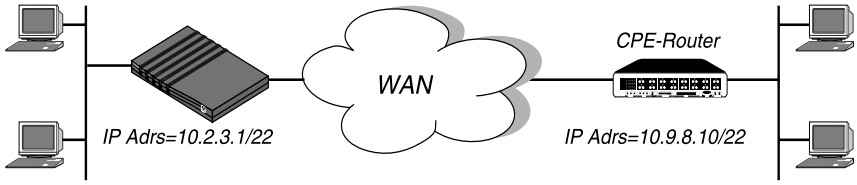


Abbildung 7-6: IP-Routing-Verbindung, die als statische Route fungiert

Hinweis: Wenn Sie im Parameter „LAN Adrs“ nicht die Netzmaske angeben, verwendet die Pipeline eine Standard-Netzmaske, bei der davon ausgegangen wird, daß auf das entfernte Netzwerk zugegriffen werden kann. Wenn die Adresse des entfernten Routers eine Netzmaske enthält, ist diese im Normalfall anzugeben.

Wenn RIP in einem Verbindungsprofil deaktiviert ist, „hört“ die Pipeline nicht auf RIP-Aktualisierungen über diese Verbindung. Um Pakete zu anderen Netzwerken über diese Verbindung zu „routen“, wird ein „Static Rtes“-Profil verwendet. Das Netzwerkdiagramm in Abbildung 7-7 zeigt ein entferntes

Netzwerk, das über kein eigenes Verbindungsprofil verfügt, aber über ein bestehendes Verbindungsprofil erreicht werden kann.

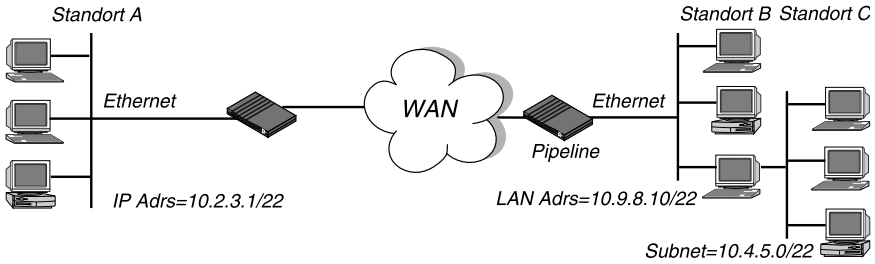


Abbildung 7-7: Verbindung über zwei Hops, die eine statische Route benötigt, wenn RIP deaktiviert wurde

In dem in Abbildung 7-7 gezeigten Beispiel-Netzwerk muß die Pipeline das folgende „Static Rtes“-Profil haben, um eine Routing-Verbindung zum Standort C herstellen zu können, falls RIP im Verbindungsprofil für Standort B deaktiviert wurde:

```
Name=Standortc-net
Active=Yes
Dest=10.4.5.6/22
Gateway=10.9.8.10
Metric=2
Private=Yes
```

Erstellen eines „Static Rtes“-Profils

„Static Rtes“-Profile können wie folgt konfiguriert werden:

1. Öffnen Sie das Menü „Static Rtes“.
2. Öffnen Sie ein „Static Rtes“-Profil.
3. Weisen Sie der Route einen Namen zu.

   Beispiel:

   ```
   Name=stefan-gw
   ```
4. Geben Sie an, daß die Route in die Routing-Tabelle aufgenommen werden soll.

   ```
   Active=Yes
   ```

5 Geben Sie das Zielnetzwerk an.

Beispiel:

```
Dest=10.210.1.30/12
```

Die Pipeline muß über ein Verbindungsprofil verfügen, in dem diese Adresse angegeben ist.

Wenn diese Adresse eine Netzmaske beinhaltet, wird der entfernte Router als Gateway zu diesem Subnetz, und nicht zu einem ganzen entfernten Netzwerk, angesehen. Soll das ganze entfernte Netzwerk angegeben werden, ist eine Netzwerkadresse wie die folgende zu verwenden:

```
Dest=10.0.0.0
```

6 Geben Sie die Adresse des Routers an, der für dieses Ziel verwendet werden soll.

Beispiel:

```
Gateway=10.9.8.10
```

Dieser Parameter legt fest, daß der Pfad zum Ziel-Subnetz über den IP-Router mit der Adresse 10.9.8.10 verläuft.

7 Geben Sie mit Hilfe des Parameters „Metric“ eine Metrik für diese Route an.

Beispiel:

```
Metric=1
```

RIP verwendet Distanzvektormetriken, d. h., die Metrik wird ähnlich wie ein Hop-Wert interpretiert. Wenn die Pipeline mehr als eine mögliche Route zu einem Zielnetzwerk hat, wählt sie die Route mit der niedrigeren Metrik.

8 Geben Sie an, ob die Route privat sein soll.

Beispiel:

```
Private=No
```

Mit dieser Einstellung wird festgelegt, daß die Pipeline die Existenz der Route angibt, wenn sie von RIP oder einem anderen Routing-Protokoll befragt wird.

9 Schließen Sie das „Static Rtes“-Profil.

Konfigurieren der Standard-Route

Wenn es zur Zieladresse eines Pakets keine Routen gibt, leitet die Pipeline das Paket an die Standard-Route weiter. Die meisten Standorte nutzen die Standard-Route zur Festlegung eines lokalen IP-Routers (z. B. eines anderen Routers oder eines UNIX-Hosts, auf dem der Routendämon läuft). Auf diese Weise können Routing-Aufgaben auf andere Geräte abgeladen werden.

Hinweis: Wird keine Standard-Route erstellt, sondert die Pipeline die Pakete, für die keine Route vorhanden ist, aus. Als Standard-Gateway verwendet die Pipeline den Wert, den Sie für den Parameter „Rem Adr“ im „Configure“-Profil angegeben haben.

Zum Konfigurieren der Standard-Route ist wie folgt vorzugehen:

1. Öffnen Sie das Menü „Static Rtes“.
2. Öffnen Sie das erste „Static Rtes“-Profil.

   Der Name dieses Profils lautet immer „Default“, und seine Zieladresse ist immer 0.0.0.0 (diese Werte können nicht geändert werden).
3. Geben Sie an, daß die Route in die Routing-Tabelle aufgenommen werden soll.

   ```
   Active=Yes
   ```
4. Geben Sie die Adresse des Routers an, der für Pakete verwendet werden soll, deren Ziel unbekannt ist.

   Beispiel:

   ```
   Gateway=10.9.8.10
   ```
5. Geben Sie eine Metrik für diese Route an.

   Beispiel:

   ```
   Metric=1
   ```
6. Geben Sie an, ob die Route privat sein soll.

   Beispiel:

   ```
   Private=Yes
   ```

   Mit dieser Einstellung wird festgelegt, daß die Pipeline die Existenz der Route angibt, wenn sie von RIP oder einem anderen Routing-Protokoll befragt wird.
7. Schließen Sie das „Static Rtes“-Profil.

Aktivieren des dynamischen Routings für die Pipeline

Die Pipeline kann Routen auf zweierlei Art und Weise „lernen“:

- RIP
- ICMP-Redirects

ICMP-Redirects

ICMP bestimmt dynamisch die beste IP-Route zu einem Zielnetzwerk oder Host und verwendet ICMP-Redirect-Pakete, um Pakete auf eine effektivere Route umzuleiten. Die Verwendung von ICMP-Redirect-Paketen ist nicht nur eines der ältesten Routenfindungsverfahren im Internet, sondern auch eines der unsichersten, ist es doch möglich, ICMP-Redirects zu fälschen. Wir empfehlen, die Pipeline so zu konfigurieren, daß ICMP-Redirects ignoriert werden.

Um die Pipeline so einzustellen, daß sie ICMP-Redirects ignoriert, ist wie folgt vorzugehen:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Stellen Sie den Parameter „ICMP Redirects“ so ein, daß keine Redirect-Pakete angenommen werden.

```
ICMP Redirects=Ignore
```

3 Schließen Sie das Ethernet-Profil.

Verwendung von RIP-1

Die Internet Engineering Task Force (IETF) hat RIP-1 inzwischen als „historisch“ eingestuft. Die Verwendung von RIP-1 wird nicht mehr empfohlen. Wir empfehlen, alle Router und Hosts auf RIP-2 aufzurüsten. Muß RIP-1 dennoch erhalten bleiben, sollte ein separates Subnetz für die RIP-1-Router und -Hosts eingerichtet werden.

Hinweis: Die Parameter „RIP Policy“ und „RIP Summary“ sind nur für RIP-1 relevant. Wir empfehlen, bei der Arbeit mit RIP-2-Routern für diese Parameter keine Werte festzulegen.

Wenn sich die Ethernet-Schnittstelle der Pipeline in einem RIP-1-Subnetz befindet, ist wie folgt vorzugehen:

1. Öffnen Sie „Ethernet-->Mod Config“.
2. Öffnen Sie das Untermenü „Ether Options“.
3. Aktvieren Sie RIP-1.

   Beispiel:

   ```
   RIP=Both-v1
   ```

   Bei dieser Einstellung sendet und empfängt die Pipeline RIP-1-Aktualisierungen im lokalen Ethernet. Soll die Pipeline nicht über lokale Routing-Änderungen informiert werden (z. B. wenn der gesamte lokale Routing-Verkehr von einem Standard-Router übernommen wird), können Sie statt dessen die folgende Einstellung verwenden:

   ```
   RIP=Send-v1
   ```

   Möchten Sie nicht, daß die Pipeline ihre WAN-Verbindungen an die RIP-1-Router im lokalen Subnetz weiterleitet, ist folgendes festzulegen:

   ```
   RIP=Roecv=v1
   ```

4. Legen Sie für „Ignor Def Rte“ den Wert „Yes“ fest.

   Mit der Standard-Route wird eine statische Route zu einem anderen IP-Router festgelegt, bei dem es sich oftmals um einen lokalen Router oder eine andere Pipeline handelt. Wenn dieser Parameter den Wert „Yes“ zugewiesen bekommt, wird die Standard-Route in der Routing-Tabelle der Pipeline nicht durch RIP-Aktualisierungen modifiziert. Wir empfehlen, mit dieser Einstellung zu arbeiten.
5. Schließen Sie das Ethernet-Profil.

Konfigurieren von RIP im Ethernet-Profil

Zum Aktivieren von RIP im lokalen Ethernet ist wie folgt vorzugehen:

1. Öffnen Sie „Ethernet-->Mod Config“.
2. Öffnen Sie das Untermenü „Ether Options“.
3. Aktivieren Sie den Parameter „RIP“.

   Beispiel:

   ```
   RIP=Both-v2
   ```

   Bei dieser Einstellung sendet und empfängt die Pipeline RIP-2-Aktualisierungen im lokalen Ethernet. Soll die Pipeline nicht über lokale Routing-Änderungen informiert werden (z. B. wenn der gesamte lokale

Routing-Verkehr von einem Standard-Router übernommen wird), können Sie statt dessen die folgende Einstellung verwenden:

```
RIP=Send-v2
```

4 Legen Sie für „Ignor Def Rte“ den Wert „Yes“ fest.

Mit der Standard-Route wird eine statische Route zu einem anderen IP-Router festgelegt, bei dem es sich oftmals um einen lokalen Router oder eine andere Pipeline handelt. Wenn dieser Parameter den Wert „Yes“ zugewiesen bekommt, wird die Standard-Route in der Routing-Tabelle der Pipeline nicht durch RIP-Aktualisierungen modifiziert. Wir empfehlen, mit dieser Einstellung zu arbeiten.

5 Schließen Sie das Ethernet-Profil.

Konfigurieren von RIP für ankommende WAN-Verbindungen

RIP wird für die WAN-Schnittstelle häufig deaktiviert, da es zu sehr großen lokalen Routing-Tabellen führen kann. Wenn RIP so eingestellt wird, daß RIP-Aktualisierungen über die WAN-Schnittstelle sowohl gesendet als auch empfangen werden können, sendet die Pipeline ihre Routing-Tabelle an das entfernte Netzwerk und wartet auf RIP-Aktualisierungen von dort. Schritt für Schritt verfügen alle Router in beiden Netzwerken über konsistente Routing-Tabellen (die alle relativ groß werden können).

Zum Konfigurieren des Antwortprofils für RIP- und IP-Routing ist wie folgt vorzugehen:

1 Öffnen Sie das „Answer“-Profil.

2 Öffnen Sie das Untermenü „PPP Options“.

3 Aktivieren Sie das IP-Routing.

```
Route IP=Yes
```

4 Öffnen Sie das Untermenü „Session Options“.

5 Aktivieren Sie den Parameter „RIP“.
Beispiel:

```
RIP=Recv-v2
```

Bei dieser Einstellung empfängt die Pipeline RIP-2-Aktualisierungen über ankommende Verbindungen mit einem anderen IP-Router. Soll der Empfang von RIP-Aktualisierungen im WAN verhindert werden, ist folgendes einzustellen:

```
RIP=Off
```

6 Schließen Sie das Antwortprofil.

Konfigurieren von RIP für eine bestimmte Verbindung

Sie können RIP für eine bestimmte Verbindung aktivieren, indem Sie das Verbindungsprofil entsprechend konfigurieren.

Hinweis: Da RIP-Aktualisierungen alle 30 Sekunden gesendet werden, sollten Sie WAN-Verbindungen, die RIP verwenden, mit einem „Idle“-Wert von unter 30 konfigurieren oder einen Ruffilter für RIP-Aktualisierungen über das WAN einrichten. Andernfalls werden diese Verbindungen nie beendet, da der RIP-Verkehr den „Idle“-Timer immer wieder zurücksetzt.

Zum Konfigurieren eines Verbindungsprofils für RIP und IP-Routing ist wie folgt vorzugehen:

1 Öffnen Sie das „Connections“-Profil.

2 Aktivieren Sie das IP-Routing.

```
Route IP=Yes
```

3 Öffnen Sie das Untermenü „IP Options“.

4 Aktivieren Sie den Parameter „RIP“.
Beispiel:

```
RIP=Recv-v2
```

Bei dieser Einstellung empfängt die Pipeline RIP-2-Aktualisierungen von dem anderen IP-Router.

Wenn der entfernte Router mit RIP-1 betrieben wird, während das lokale Netzwerk mit RIP-2 arbeitet, oder Sie einfach nicht wollen, daß die Pipeline über diese Verbindung RIP-Aktualisierungen sendet oder empfängt, ist die folgende Einstellung zu verwenden:

```
RIP=None
```

5 Schließen Sie das Verbindungsprofil.

Routenpräferenzen

Bei der Bestimmung, welche Routen in die Routing-Tabelle aufgenommen werden sollen, vergleicht der Router zunächst die Präferenzwerte und wählt die niedrigere Nummer. Sind die Präferenzwerte gleich, vergleicht der Router als nächstes die Werte des Parameters „Metric“ und entscheidet sich für die Route mit der niedrigeren Metrik.

Gibt es für eine bestimmte Adresse und Netzmaske mehrere Routen, ist die Route mit dem geringeren Präferenzwert vorzuziehen. Wenn zwei Routen den gleichen Präferenzwert haben, wird der Route mit dem niedrigeren „Metric“-Wert der Vorzug gegeben. Der Router verwendet letztendlich die nach diesen Kriterien vorzuziehende Route. Die anderen Routen bleiben latent bzw. „verborgen“ und kommen zum Einsatz, wenn die jeweils beste Route nicht mehr verfügbar ist.

Für die Standard-Route gelten die folgenden Präferenzwerte:

- verbundene Routen, wie z. B. Ethernet: „Preference=0“
- über ICMP-Redirects erlernte Routen: „Preference=30“
- statische Routen: „Preference=100“
  Diesen Standardwert können Sie im Verbindungs- bzw. „Static Rtes“-Profil ändern.
- von RIP erlernte Routen: „Preference=100“
- Routen, die der Tabelle durch die SNMP-MIB II hinzugefügt wurden: „Preference=100“

Festlegen der Routenpräferenzen für eine WAN-

Verbindung

Die statische Route in einem Verbindungs- oder „Static Rtes“-Profil hat standardmäßig einen Präferenzwert von 100. Bei diesem Wert haben statische Routen und RIP-Routen den gleichen Wert, wobei ICMP-Redirects (falls von der Einheit akzeptiert) beiden Routenarten vorgezogen werden.

Um zum Beispiel festzulegen, daß die in einem Verbindungsprofil konfigurierte statische Route einer Route zum selben Ziel vorgezogen wird, die über ein RIP-Broadcast in die Tabelle aufgenommen wurde, ist wie folgt vorzugehen:

1. Öffnen Sie das „Connections“-Profil.
2. Öffnen Sie das Untermenü „IP Options“.
3. Geben Sie für den Parameter „Preference“ einen niedrigeren Wert als 100 an. Beispiel:

   ```
   LAN Adrs=10.9.8.10/22
   WAN Alias=0.0.0.0
   Metric=5
   Preference=50
   Private=No
   RIP=Off
   ```

4. Schließen Sie das Ethernet-Profil.

Anzeigen der Routing-Tabelle

Der Terminal-Server-Befehl „IPROUTE SHOW“ enthält Informationen, die für mehrere IP-Routing-Protokolle relevant sind. Sie können sich die IP-Routing-Tabelle anzeigen lassen, indem Sie die Terminal-Server-Schnittstelle aufrufen und an der Eingabeaufforderung den folgenden Befehl eingeben:

```
iproute show
```

Daraufhin erscheint auf dem Bildschirm eine Tabelle, die der folgenden ähnelt:

```
Destination        Gateway        IF       Flg Pref  Met   Use   Age
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
10.207.76.1/32     10.207.76.1    wanidle0 S    100   7     2     20887
```

```
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
127.0.0.1/32       -              lo0      CP   0     0     0     20887
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
10.0.0.100/32      10.0.0.100     wan0     S    100   1     153   20887
10.1.2.0/24        -              ie0      C    0     0     19775 20887
10.1.2.1/32        -              lo0      CP   0     0     389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

Diese Tabelle enthält die folgenden Routen:

```
0.0.0.0/0      10.0.0.100     wan0     SG   1     1     0
20887
```

Dies ist die Standard-Route; sie weist durch das aktive Verbindungsprofil. Im „Static Rtes“-Profil für die Standard-Route ist ein „Preference“-Wert von 1 festgelegt, so daß dieser Route gegenüber dynamisch erlernten Routen der Vorzug gegeben wird.

```
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0
20887
10.207.76.1/32       10.207.76.1    wanidle0 S    100   7     2
20887
```

Diese Routen sind in einem Verbindungsprofil festgelegt. Beachten Sie, daß es sich um zwei Routen handelt – eine direkte Route zum Gateway und eine Route zum größeren Netzwerk.

```
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0
20887
```

Dies ist eine statische Route, die durch ein inaktives Gateway weist.

```
127.0.0.1/32       -              lo0      CP   0     0     0
20887
```

Dies ist eine Loopback-Route, die bewirkt, daß Pakete an diese spezielle Adresse intern bearbeitet werden. Das Flag „C“ gibt an, daß es sich um eine verbundene Route („Connected“) handelt, während mit dem Flag „P“ („Private“) angegeben wird, daß der Router diese Route nicht bekanntmacht.

```
10.0.0.0/24    10.0.0.100 wan0     SG   100   1     21387 20887
10.0.0.100/32    10.0.0.100   wan0       S     100    1      153
   20887
```

Diese Routen werden durch ein gegenwärtig aktives Verbindungsprofil angelegt. Sie sind den oben gezeigten 10.207.76.0-Routen ähnlich, weisen aber durch ein aktives Gateway.

```
10.1.2.0/24    -              ie0      C    0     0     19775 20887
```

Diese Route beschreibt die Verbindung zur Ethernet-Schnittstelle. Es handelt sich bei ihr um eine direkt verbundene Route mit einem „Preference“- und einem „Metric“-Wert von jeweils 0.

```
10.1.2.1/32    -              lo0      CP   0     0     389   20887
```

Dies ist eine weitere Loopback-Route, und zwar eine Host-Route mit unserer Ethernet-Adresse. Da sie eine private Route ist, wird sie nicht bekanntgemacht.

```
255.255.255.255/32 -              ie0      CP   0     0     0
20887
```

Dies ist eine private Route zur Broadcast-Adresse. Diese Route wird dann verwendet, wenn der Router ein Broadcast-Paket senden will, aber sonst nicht konfiguriert ist. Ein typisches Einsatzgebiet für eine solche Route ist die Suche nach einem Server auf einem Client-Computer, der Abfragen für eine Token-Sicherheitskarte bearbeitet.

Beschreibung der Felder in der Routing-Tabelle

Die Spalten in der Routing-Tabelle zeigen die folgenden Informationen an:

- „Destination“
  Die Spalte „Destination“ gibt die Zieladresse der Route an. Um ein Paket an diese Adresse zu senden, verwendet die Pipeline diese Route. Dabei ist zu beachten, daß der Router die am meisten spezifizierte Route (die Route mit der größten Netzmaske) verwendet, die dem angegebenen Ziel entspricht.
- „Gateway“
  In der Spalte „Gateway“ wird die Adresse des nächsten Routers angegeben, der Pakete an ein bestimmtes Ziel weiterleiten kann. Für direkte Routen (ohne Gateway) wird in der Spalte „Gateway“ kein Gateway mehr angezeigt.

- „IF“
  Die Spalte „IF“ („Interface“) zeigt den Namen der Schnittstelle an, durch die ein Paket mit dieser Adresse gesendet wird.
  - „ie0“ ist die Ethernet-Schnittstelle
  - „lo0“ ist die Rückschleifen-Schnittstelle
  - „wanN“ gibt die Nummer der aktiven WAN-Schnittstelle an
  - „wanidle0“ ist die inaktive Schnittstelle (die spezielle Schnittstelle, auf die alle Routen gerichtet sind, wenn ihre WAN-Verbindungen „down“ sind).
- „Flg“
  Die Spalte „Flg“ („Flag“) kann die folgenden Flag-Werte enthalten:
  - C – „Connected“ (direkt verbundene Route, z. B. das Ethernet)
  - I – ICMP (dynamische ICMP-Redirect-Route)
  - N – „NetMgt“ (über SNMP-MIB II in die Tabelle aufgenommen)
  - R – RIP (dynamische RIP-Route)
  - S – „Static“ (lokal in einem „Static Rtes“- oder Verbindungsprofil konfigurierte Route)
  - ? – Unbekannt (Route mit unbekanntem Fehler; zeigt einen Fehler an)
  - G – „Gateway“ (diese Route kann nur über ein Gateway erreicht werden)
  - P – „Private“ (diese Route wird nicht über RIP bekanntgemacht)
  - T – „Temporary“ (diese Route wird zerstört, wenn ihre Schnittstelle nicht mehr verfügbar ist)
  - * – verborgen (Wenn eine Route verborgen ist, heißt das, daß es eine bessere Route in der Tabelle gibt, so daß diese Route „hinter“ der besseren Route verborgen ist. Ist die bessere Route nicht mehr verfügbar, kann statt dessen diese Route verwendet werden.)
- „Pref“
  Die Spalte „Pref“ („Preference“) enthält den Präferenzwert der Route. Alle Routen, die über RIP in die Tabelle aufgenommen werden, haben einen festen Präferenzwert von 100. Der Präferenzwert der statischen Routen kann dagegen unabhängig festgesetzt werden. Siehe dazu „Routenpräferenzen“ auf Seite 7-33.

- „Metric“
  In der Spalte „Metric“ wird die in RIP-Form angegebene Metrik für die Route angezeigt, wobei der gültige Bereich von 0 bis 16 geht.
- „Use“
  In dieser Spalte wird angezeigt, wie häufig die Route seit ihrer Erstellung verwendet wurde. (Viele dieser Verwendungen sind intern, so daß sich aus dieser Zahl nicht die Anzahl der Pakete erkennen läßt, die über diese Route gesendet wurden.)

  Hinweis: Für Routen, die nicht benutzt wurden, wird in der Spalte „Use“ der Wert 0 angezeigt.
- „Age“
  In dieser Spalte wird das Alter der Route in Sekunden angezeigt. Anhand dieses Wertes lassen sich Probleme erkennen, wenn Routen sich schnell ändern oder „flattern“.

Konfigurieren von IP-Routing-Verbindungen

In diesem Abschnitt wird die Konfiguration von IP-Routing-Verbindungen beschrieben. Nachdem auf die Anforderungen an die Host-Software eingegangen wurde, werden die folgenden Beispielkonfigurationen beschrieben:

- Beispiel für eine Host-Verbindung mit statischer Adresse
- Beispiel für eine Router-Verbindung
- Beispiel für eine Router-Verbindung in einem Subnetz

Hinweis: Der häufigste Fehler beim Erstaufbau einer IP-Verbindung ist die falsche Konfiguration der IP-Adresse oder Subnetzmaske für den entfernten Host bzw. das rufende Gerät.

Für den entfernten Host erforderliche Software

IP-Hosts, wie UNIX-Systeme, Windows- oder OS/2-PCs oder Macintosh-Systeme, müssen über entsprechend konfigurierte TCP/IP-Software verfügen. Ein entfernter Host, der sich in das lokale IP-Netzwerk einwählt, muß auch PPP-Software haben.

- UNIX

  UNIX-Systeme verfügen im Normalfall über einen TCP/IP-Stack, DNS-Software und andere Programme, Dateien und Utilities für die Internet-Kommunikation. Die Konfiguration dieser Programme und Dateien wird in der Dokumentation zur UNIX-Netzwerkadministration beschrieben.

- PC-kompatible Hosts

  PCs unter Windows oder OS/2 benötigen die TCP/IP-Netzwerk-Software („Stack“) . In Windows 95 ist der Stack bereits enthalten, für frühere Windows-Versionen bzw. für OS/2 muß er aber zumeist extra erworben und installiert werden.

- Macintosh

  Macintosh-Computer benötigen für den Einsatz von TCP/IP entweder MacTCP oder Open Transport. MacTCP ist bereits Bestandteil aller Apple-Betriebssysteme ab Version 7.1. Diese Software (MacTCP oder MacTCP Admin) befindet sich, wenn installiert, im Ordner „Kontrollfelder“.

Bei allen Plattformen muß die TCP/IP-Software mit der IP-Adresse und der Subnetzmaske für den Host konfiguriert werden. Bezieht der Host seine IP-Adresse von der Pipeline auf dynamischem Wege, muß die TCP/IP-Software so konfiguriert werden, daß eine dynamische Zuweisung erfolgen kann. Wird in Ihrem lokalen Netzwerk ein DNS-Server unterstützt, ist die Host-Software mit der Adresse des DNS-Servers zu konfigurieren.

Im Normalfall wird die Host-Software so konfiguriert, daß die Pipeline als Standard-Router agiert.

Beispiel für eine Host-Verbindung mit einer statischen Adresse

Eine Host-Routen-Verbindung ermöglicht es dem Einwählhost, beim Einloggen in das IP-Netzwerk der Pipeline seine eigene IP-Adresse zu behalten. Wenn zum Beispiel ein PC-Benutzer sich bei einem IP-Netzwerk anmeldet und einen ISP in einem anderen IP-Netzwerk verwendet, kann eine dieser Verbindungen eine IP-Adresse zuweisen, während die andere eine Host-Route zum PC konfigurieren kann. Das folgende Beispiel zeigt, wie bei der Konfiguration einer Host-Route vorzugehen ist. Näheres zur /32-Netzmaske finden Sie im Abschnitt „Die Ascend-Netzmaskenkonvention“ auf Seite 7-5.

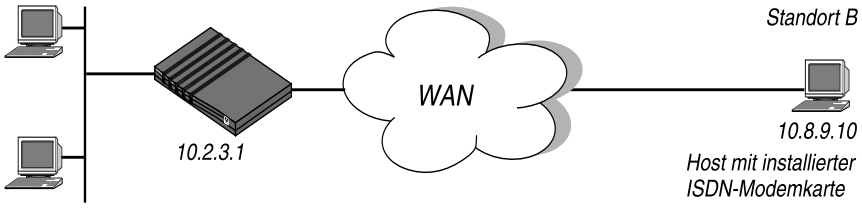


Abbildung 7-8: Benutzer, der sich einwählt und dafür eine statische IP-Adresse (Host-Route) benötigt

In diesem Beispiel läuft auf dem PC am Standort B, an den eine ISDN-Modemkarte angeschlossen ist, PPP-Software und der TCP/IP-Stack. Die PPP-Software beinhaltet z. B. die folgenden Einstellungen:

```
Username=Simon
Accept Assigned IP=N/A (oder „No“)
IP Address=10.8.9.10
Netmask=255.255.255.255
Default Gateway=N/A (oder „None“)
Name Server=10.7.7.1
Domain suffix=abc.com
VAN Jacobsen compression ON
```

Um die Pipeline so zu konfigurieren, daß sie vom Standort B initiierte Verbindungen akzeptiert, ist wie folgt vorzugehen:

1 Öffnen Sie das „Answer“-Profil.

2 Aktivieren Sie das IP-Routing.

```
Route IP=Yes
```

3 Schließen Sie das Antwortprofil.

4 Öffnen Sie das „Connections“-Profil für den sich einwählenden Benutzer.

5 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Station=Simon
Active=Yes
Encaps=PPP
Route IP=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*

IP options...
    LAN Adrs=10.8.9.10/32
    RIP=Off
```

6 Schließen Sie das Verbindungsprofil.

Beispiel für eine Router-Verbindung

In diesem Beispiel ist die Pipeline mit einem IP-Netzwerk im Unternehmen verbunden und benötigt eine gewählte Verbindung zu einem anderen Unternehmen, das über eine eigene IP-Konfiguration verfügt. Abbildung 7-9 zeigt ein Beispiel-Netzwerkdiagramm.

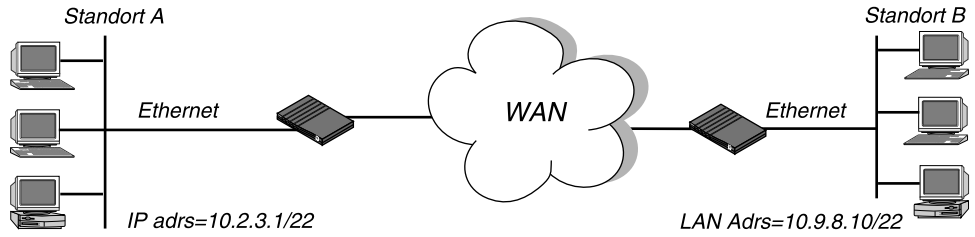


Abbildung 7-9: IP-Verbindung von Router zu Router

Bei diesem Beispiel wird davon ausgegangen, daß das Antwortprofil und das Ethernet-Profil in beiden Geräten so konfiguriert wurden, daß sie IP-Routing erlauben.

Um die Pipeline an Standort A für eine Verbindung mit Standort B zu konfigurieren, ist wie folgt vorzugehen:

1 Öffnen Sie das entsprechende „Connections“-Profil.

2 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Station=PipelineB
Active=Yes
Encaps=MPP
Route IP=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IP options...
    LAN Adrs=10.9.8.7/22
    RIP=Send-v2
```

3 Schließen Sie das „Connections“-Profil.

Konfigurieren der Pipeline an Standort B:

1 Öffnen Sie das entsprechende „Connections“-Profil.

2 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Station=PipelineA
Active=Yes
Encaps=MPP
Route IP=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IP options...
    LAN Adrs=10.2.3.1/22
    RIP=Recv-v2
```

3 Schließen Sie das „Connections“-Profil.

Beispiel für eine Router-Verbindung in einem Subnetz

In diesem Beispiel-Netzwerk wird die Pipeline verwendet, um Telearbeiter mit eigenen Ethernet-Netzwerken mit dem Unternehmensnetzwerk zu verbinden. Die Pipeline befindet sich in einem Subnetz und weist den Telearbeiter-Netzwerken Subnetzadressen zu.

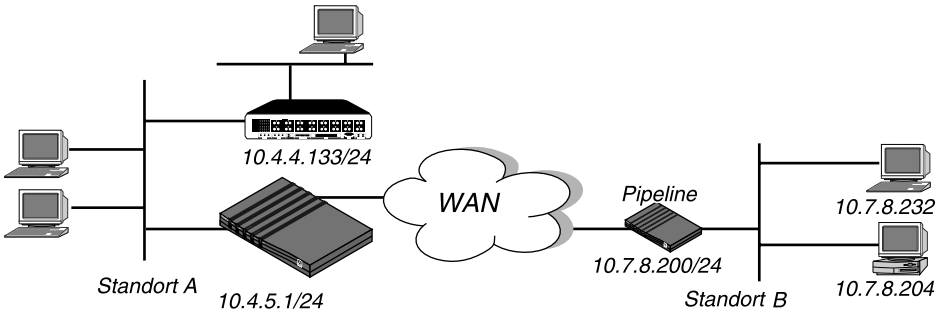


Abbildung 7-10: Verbindung zwischen lokalen und entfernten Subnetzen

Bei diesem Beispiel wird davon ausgegangen, daß bei beiden Geräten sowohl im „Answer“-Profil als auch im Ethernet-Profil das IP-Routing aktiviert ist.

Da die Pipeline als Teil ihrer eigenen IP-Adresse eine Netzmaske spezifiziert, muß sie für die Weiterleitung von Paketen an IP-Adressen außerhalb ihres Subnetzes andere Router verwenden. Um Pakete an andere Teile des Unternehmensnetzes senden zu können, muß für die Pipeline entweder eine Standard-Route zu einem Router in ihrem eigenen Subnetz, wie z. B. dem in Abbildung 5-12 gezeigten Cisco-Router, konfiguriert haben, oder in ihrem Ethernet-Profil muß RIP aktiviert sein.

Um die Pipeline an Standort A für eine Verbindung mit Standort B zu konfigurieren, ist wie folgt vorzugehen:

1 Öffnen Sie das „Connections“-Profil.

2 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Station=PipelineX
Active=Yes
Encaps=MPP
Route IP=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IP options...
    LAN Adrs=10.7.8.200/24
    RIP=Off
```

3 Schließen Sie das „Connections“-Profil.

4 Öffnen Sie das „Static Rtes“-Profil „Default“.

5 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Name=Default
Active=Yes
Dest=0.0.0/0
Gateway=10.4.4.133/24
Metric=1
Preference=100
Private=Yes
```

6 Schließen Sie das „Static Rtes“-Profil.

Konfigurieren der Pipeline an Standort B:

7 Öffnen Sie das entsprechende „Connections“-Profil.

8 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Station=PipelineA
Active=Yes
Encaps=MPP
Route IP=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IP options...
    LAN Adrs=10.4.5.1/24
    RIP=Off
```

9 Schließen Sie das „Connections“-Profil.

10 Öffnen Sie das „Static Rtes“-Profil „Default“ (in der Pipeline an Standort B).

11 Legen Sie die Einstellungen für die folgenden Parameter fest:

```
Name=Default
Active=Yes
Dest=0.0.0/0
Gateway=10.4.5.1/24
Metric=1
Preference=100
Private=Yes
```

Schließen Sie das „Static Rtes“-Profil.

Konfigurieren der Pipeline als IPX-Router

8

Dieses Kapitel enthält die folgenden Abschnitte:

Die Pipeline als IPX-Router – Einführung

In dieser Einführung wird beschrieben, wie die Pipeline IPX-Routing zwischen Standorten unterstützt, die mit Novell NetWare 3.11 oder höher arbeiten. Die Pipeline operiert als IPX-Router mit einer Schnittstelle zum lokalen Ethernet und einer anderen Schnittstelle zum WAN. Die IPX-Verbindungsprofile agieren als IPX-WAN-Schnittstelle.

IPX-Routing wird in der Pipeline vor allem zu den folgenden Zwecken eingesetzt:

- Integration mehrerer NetWare-LANs zur Bildung eines WANs aus mehreren miteinander verbundenen Netzwerken
- Ermöglichung des Zugriffs auf lokale NetWare-Dienste durch sich einwählende NetWare-Clients

Die Pipeline unterstützt IPX-Routing über PPP-, MP-, und Frame-Relay-Verbindungen. Durch die Unterstützung der Protokolle IPXWAN und PPP IPXCP ist die Pipeline uneingeschränkt zusammen mit nicht von Ascend stammenden Produkten einsetzbar, die diesen Protokollen und den entsprechenden RFCs entsprechen.

Hinweis: IPX-Pakete können mit verschiedenen Rahmentypen transportiert werden. Die Pipeline kann nur einen IPX-Rahmentyp „routen“, und IPX-Pakete werden nur „geroutet“ oder „gespooft“, wenn sie mit diesem Rahmentyp versehen sind. Wenn in ein und demselben Verbindungsprofil Bridging und IPX-Routing aktiviert ist, „bridgt“ die Pipeline alle Pakete, die einen anderen IPX-Rahmentyp haben. Weitere Informationen dazu finden Sie im Kapitel 6, „Konfigurieren der Pipeline als Bridge“.

Im Gegensatz zu IP-Routing-Konfigurationen, bei denen die Pipeline das rufende Gerät eindeutig an dessen IP-Adresse erkennt, gibt es beim IPX-Routing keine „eingebaute“ Methode, die rufende Seite eindeutig zu bestimmen. Daher muß mit Kennwort-Authentifizierung mit PAP bzw. CHAP gearbeitet werden, wenn nicht im selben Verbindungsprofil auch IP-Routing aktiviert wurde. Siehe dazu Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

IPX-SAP-Tabellen

Die Pipeline zeigt das Standard-IPX-SAP-Verhalten (Service Advertising Protocol) für Router. Ist sie jedoch mit einer anderen Ascend-Einheit verbunden, die ebenfalls für IPX-Routing konfiguriert ist, tauschen beide Seiten der Verbindung ihre gesamten SAP-Tabellen aus, so daß alle entfernten Dienste direkt in die SAP-Tabelle der Pipeline aufgenommen werden.

NetWare-Server senden alle 60 Sekunden SAP-Pakete, um die Router (wie z. B. die Pipeline) über ihre Dienste zu informieren. Router erstellen eine SAP-Tabelle mit einem Eintrag für jeden Dienst, der von einem bekannten Server bekanntgemacht wird. Wenn ein Router keine SAP-Broadcasts mehr von einem bestimmten Server empfängt, wird der Eintrag nach einiger Zeit aus der SAP-Tabelle entfernt.

Die SAP-Tabellen werden von Routern benutzt, um auf Client-Abfragen antworten zu können. Wenn ein NetWare-Client eine SAP-Anforderung sendet, um nach einem Dienst zu suchen, überprüft die Pipeline ihre SAP-Tabelle und antwortet mit ihrer eigenen Hardware-Adresse sowie der internen Adresse des angeforderten Servers. Dies ist analog zum Proxy-ARP-Modus beim IP-Routing.

Der Client kann dann Pakete senden, deren Zieladresse die interne Adresse des Servers ist. Wenn die Pipeline diese Pakete empfängt, überprüft sie ihre RIP-Tabelle. Findet sie dort einen Eintrag für diese Zieladresse, stellt sie die Verbindung her bzw. leitet das Paket über die aktive Verbindung weiter.

IPX-RIP-Tabellen

Die Pipeline zeigt beim Aufbau von Verbindungen zu nicht von Ascend stammenden Einheiten das Standard-IPX-RIP-Verhalten (Routing Information Protocol) für Router. Ist sie jedoch mit einer anderen Ascend-Einheit verbunden, die ebenfalls für IPX-Routing konfiguriert ist, tauschen beide Seiten der Verbindung sofort ihre gesamten RIP-Tabellen aus. Außerdem erhält die Pipeline die RIP-Einträge solange als statisch aufrecht, bis die Einheit zurückgesetzt oder neu eingeschaltet wird.

IPX RIP ähnelt dem Protokoll für Routing-Informationen, das Teil der TCP/IP-Protokollsammlung ist; es handelt sich aber um ein eigenes Protokoll. In diesem Kapitel ist mit RIP immer IPX RIP gemeint.

Das Ziel einer IPX-Route ist das interne Netzwerk eines Servers. So wird zum Beispiel NetWare-Dateiservern vom Netzwerkadministrator eine interne IPX-Netzwerknummer zugewiesen, und sie haben sehr häufig die Standard-Knotenadresse 000000000001. Dies ist die Zielnetzwerkadresse für Anforderungen zum Lesen und Schreiben von Dateien. (Nähere Informationen zu den internen Netzwerknummern finden Sie in Ihrer NetWare-Dokumentation.)

IPX-Router senden in regelmäßigen Abständen und nach der Errichtung einer WAN-Verbindung RIP-Aktualisierungen. Die Pipeline empfängt RIP-Broadcasts von einem entfernten Gerät, erhöht den Hop-Wert für jede bekanntgemachte Route um 1, aktualisiert ihre eigene RIP-Tabelle und sendet die RIP-Pakete im Split-Horizon-Verfahren über erreichbare Netzwerke.

Die Pipeline erkennt die Netzwerknummer –2 (0xFFFFFFFE) als IPX-RIP-Standard-Route. Wenn sie ein Paket für ein unbekanntes Ziel empfängt, leitet sie das Paket an den IPX-Router weiter und bietet die Standard-Route an. Wenn die Standard-Route von mehreren IPX-Routern angeboten wird, wird die Route entsprechend den jeweiligen Hop- und Tick-Werten festgelegt. Empfängt die Pipeline z. B. ein IPX-Paket, das für das Netzwerk mit der Nummer 77777777 bestimmt ist, und gibt es in der RIP-Tabelle keinen Eintrag für dieses Ziel, leitet die Pipeline das Paket an die Netzwerknummer FFFFFFFE weiter, wenn diese verfügbar ist, statt es einfach auszusondern.

Ascend-Erweiterungen des Standard-IPX

NetWare arbeitet mit dynamischen Routing- und Dienstorten, so daß Clients davon ausgehen, daß sie einen Server dynamisch finden können, egal welche physikalische Position dieser hat. Dieses Merkmal wurde für die Arbeit in LAN-Umgebungen entwickelt, und nicht für WANs. Um einen Einsatz im WAN zu ermöglichen, stellt Ascend die folgenden Erweiterungen des Standard-IPX zur Verfügung:

- „Dial Query“
- Watchdog-Spoofing
- Definition eines virtuellen IPX-Netzwerks für Einwähl-Clients
- IPX-Routing-Profile
- IPX-SAP-Filter

Tabelle 8-1 zeigt die Parameter für die Ascend-IPX-Erweiterungen:

Tabelle 8-1: Ascend-Erweiterungen des Standard-IPX-Routings

Ort	**Parameter mit Beispielwerten**
Ethernet > Connections > *alle Profile* > IPX options... (Verbindungsprofil)	Peer=Dialin *(dynamische Adressierung)* IPX RIP=None IPX SAP=Send Dial Query=No Handle IPX=Client *(IPX-Client-Bridging)* Netware t/o=30 *(Watchdog-Spoofing)*
Ethernet > Mod Config > Ether options... (Ethernet-Profil)	IPX Pool #=CFCF1234
Ethernet > IPX-Routen > *alle Profile* (IPX-Routing-Profil)	Server Name=*Servername* Active=Yes Network=CC1234FF Node=000000000001 Socket=0000 Server Type=0004 Hop Count=2 Tick Count=12 Connection #=0
Ethernet > IPX-SAP-Filter > *alle Profile* (IPX-SAP-Filterprofil)	Name=optional Input SAP filters... Output SAP filters Valid=Yes Type=Exclude Server Type=0004 Server Name=SERVER-1

Weitere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch.*

Informationen zum Parameter „Handle IPX“ und zum IPX-Bridging können Sie Kapitel 6, „Konfigurieren der Pipeline als Bridge“. entnehmen.

„Dial Query“

„Dial Query“ ist ein Verbindungsprofil-Parameter, der die Pipeline auffordert, die Verbindung aufzubauen, wenn sie eine SAP-Anforderung für den Diensttyp 0004 („File Server“) empfängt, und dieser Diensttyp in der SAP-Tabelle der Pipeline nicht eingetragen ist. Wenn die Pipeline keinen SAP-Tabelleneintrag für den Diensttyp 0004 hat, wird jede Verbindung aufgebaut, in deren Profil „Dial Query“ aktiviert wurde. Ist „Dial Query“ bei 5 Verbindungsprofilen aktiviert, baut die Pipeline also als Reaktion auf die Anfrage alle 5 Verbindungen auf.

Hinweis: Wenn in der SAP-Tabelle der Pipeline eine statische IPX-Route zu mindestens einem entfernten Server eingetragen ist, wird diese Verbindung aufgebaut, da das Herstellen jeder Verbindung, bei der „Dial Query“ aktiviert wurde, die teurere Lösung darstellt.

Watchdog-Spoofing

NetWare-Server senden NCP-Watchdog-Pakete aus, um die Client-Verbindungen zu überwachen. Clients, die auf Watchdog-Pakete reagieren, bleiben beim Server angemeldet. Wenn ein Client nicht innerhalb eines bestimmten Zeitraums auf ein Watchdog-Paket für den Server reagiert, wird der Client vom Server ausgeloggt.

Das wiederholte Senden von Watchdog-Paketen würde dazu führen, daß die WAN-Verbindung aufrechterhalten bleibt, aber wenn die Pipeline diese Pakete einfach nur filtern würde, würden die Clients vom entfernten Server ausgeloggt werden. Um das wiederholte Ausloggen von Clients zu verhindern und gleichzeitig zu gestatten, daß WAN-Verbindungen bei Inaktivität beendet werden, antwortet die Pipeline auf NCP-Watchdog-Anforderungen als Proxy für Clients auf der anderen Seite einer IPX-Routing- oder IPX-Bridging-Verbindung, die offline ist. Das Antworten auf solche Anforderungen wird im allgemeinen Watchdog-Spoofing (to spoof = hereinlegen, täuschen) genannt. Für den Server sieht eine solcherart „gespoofte“ Verbindung wie eine normale, aktive Client-Login-Verbindung aus, so daß er den Client nicht ausloggt.

Der Timer beginnt mit dem Herunterzählen, sobald die Verbindung nicht mehr besteht. Wenn die festgelegte Zeitdauer abgelaufen ist, hört die Pipeline auf, auf Watchdog-Pakete zu antworten, und die Client-Server-Verbindungen können vom Server freigegeben werden. Wird die Verbindung zum WAN vor Ablauf des festgelegten Zeitraums wiederaufgenommen, wird der Timer zurückgesetzt.

Hinweis: Die Pipeline-Software filtert IPX-Watchdog-Pakete bei allen IPX-Routing-Verbindungen und allen IPX-Bridging-Verbindungen, bei denen Watchdog-Spoofing aktiviert ist, automatisch. Die Pipeline wendet einen implizierten Ruffilter an, der verhindert, daß der „Idle“-Timer zurückgesetzt wird, wenn IPX-Watchdog-Pakete gesendet oder empfangen werden. Dieser Filter kommt nach den Standard-Daten- und Ruffiltern zum Einsatz.

Virtuelles IPX-Netzwerk für Einwähl-Clients

Die Pipeline ermöglicht es individuellen NetWare-Clients, die keine IPX-Netzwerkadresse haben, eine IPX-Routing-Verbindung zum lokalen Netzwerk zu verwenden. Beim Client muß PPP-Client-Software laufen, damit eine Verbindung mit dem IPX-Netzwerk über die Pipeline hergestellt werden kann.

Um die Pipeline in die Lage zu versetzen, Pakete zu diesen Einwähl-Clients weiterzuleiten, muß im Ethernet-Profil eine IPX-Netzwerknummer angegeben werden, die innerhalb der gesamten IPX-Routing-Domäne der Pipeline (die lokale Routing-Domäne plus alle WAN-Verbindungen) nur einmal vergeben sein darf. Dies ist ein „virtuelles“ IPX-Netzwerk, das für Einwähl-Clients reserviert ist.

Im Verbindungsprofil für die einzelnen Einwähl-Clients muß „Dialin“ festgelegt sein, damit die Pipeline bei der PPP-Verhandlung dem Einwähl-Client die virtuelle IPX-Netzwerknummer zuweist. Stellt der Client nicht seine eigene eindeutige Knotennummer zur Verfügung, weist die Pipeline auch dem Client eine eindeutige Knotennummer zu. Sie sendet keine RIP- und SAP-Bekanntmachungen über die Verbindung und ignoriert vom entfernten Ende ankommende RIP- und SAP-Bekanntmachungen. Auf RIP- und SAP-Anforderungen von Einwähl-Clients wird jedoch reagiert.

Siehe dazu „Definieren eines virtuellen IPX-Netzwerks für Einwähl-Clients“ auf Seite 8-15 und „Beispiel für eine Einwähl-Client-Verbindung“ auf Seite 8-29.

IPX-Routing-Profile

Zur Festlegung statischer IPX-Routen werden IPX-Routing-Profile verwendet. Wenn die RIP- und SAP-Tabellen der Pipeline aufgrund einer Zurücksetzung oder eines Neustarts gelöscht wurden, werden die statischen Routen hinzugefügt, sobald die Einheit initialisiert wird. Jede statische Route enthält die Informationen, die für das Erreichen eines bestimmten Servers erforderlich sind.

Wenn die Pipeline nach einer Zurücksetzung oder einem Neustart einer anderen Ascend-Einheit zum ersten Mal wieder eine Verbindung zu dieser entfernten Einheit herstellen will, und für diese Einheit keine statische Route konfiguriert ist, muß die Verbindung mit Hilfe des DO-Menüs manuell gewählt werden. Nach dem erstmaligen Herstellen der Verbindung lädt die Pipeline die RIP-Tabelle vom entfernten Standort und erhält die Routen so lange aufrecht, bis die Einheit erneut zurückgesetzt oder neu gestartet wird.

Statische Routen bedürfen einer manuellen Aktualisierung, sobald der angegebene Server nicht mehr verfügbar ist oder sich die Serveradresse geändert hat. Statische Routen stellen jedoch eine Möglichkeit dar sicherzustellen, daß die Pipeline die entsprechende Verbindung herstellen kann, wenn Clients SAP-Anforderungen senden. Außerdem können auf diese Weise Timeouts verhindert werden, wenn das Auffinden eines Servers im WAN durch einen Client zu lange dauert. Siehe dazu „Konfigurieren einer statischen IPX-Route“ auf Seite 8-19.

IPX-SAP-Filter

Viele Standorte wünschen nicht, daß die SAP-Tabelle der Pipeline lange Listen aller am entfernten Standort verfügbaren Server beinhaltet. Mit IPX-SAP-Filtern haben Sie die Möglichkeit, bestimmte Dienste explizit in die SAP-Tabelle aufzunehmen oder aus dieser auszuschließen.

SAP-Filter können sowohl für ankommende als auch abgehende SAP-Pakete eingesetzt werden. Die Filter für ankommende Pakete sorgen dafür, daß nur bestimmte der über die Netzwerkverbindung bekanntgemachten Dienste in die SAP-Tabelle der Pipeline aufgenommen werden. Mit Hilfe der Filter für abgehende Pakete kann festgelegt werden, welche Dienste die Pipeline über eine bestimmte Netzwerkverbindung bekanntmachen soll. Siehe dazu „Filter für den SAP-Verkehr“ auf Seite 8-23.

Einsatz von NetWare-Client-Software im WAN

Für den Einsatz von NetWare-Clients in einem WAN ist in den meisten Fällen keine Sonderkonfiguration erforderlich. Im folgenden werden einige der Probleme genannt, die sich für einige NetWare-Clients in IPX-Routing-Umgebungen ergeben können:

- Bevorzugte Server

Wenn das lokale IPX-Netzwerk NetWare-Server unterstützt, sollte sich der von den NetWare-Clients bevorzugte Server im lokalen Netzwerk statt an einem entfernten Standort befinden. Wenn das lokale Ethernet NetWare-Server nicht unterstützt, empfiehlt es sich, für die lokalen Clients einen bevorzugten Server in dem Netzwerk festzulegen, bei dem die geringsten Verbindungsgebühren anfallen. Weitere Informationen entnehmen Sie bitte Ihrer NetWare-Dokumentation.

- Lokale Kopie von LOGIN.EXE

  Das Starten von ausführbaren Programmen an einem entfernten Standort ist aufgrund der damit möglicherweise verbundenen Geschwindigkeitsprobleme nicht zu empfehlen. Wir empfehlen statt dessen, bei allen Clients LOGIN.EXE lokal zu installieren.

- Packet Burst (NetWare 3.11)

  „Packet Burst“ ist ein Protokoll, mit dem ein Server einen Datenstrom über das WAN senden kann, bevor vom Client eine Quittung gesendet wird. Dieses Protokoll ist in der Server- und Client-Software für NetWare 3.12 oder später automatisch enthalten. Wenn lokale Server unter NetWare 3.11 laufen, sollte auf ihnen PBURST.NLM geladen sein. Weitere Informationen dazu finden Sie in Ihrer NetWare-Dokumentation.

- Macintosh- oder UNIX-Clients

  Sowohl Macintosh- als auch UNIX-Clients können IPX für die Kommunikation mit Servern verwenden. Beide Client-Arten unterstützen aber auch native Protokolle (Macintosh: AppleTalk, UNIX: TCP/IP). Wenn Macintosh-Clients mit Hilfe von AppleTalk-Software (statt mit MacIPX) über das WAN auf NetWare-Server zugreifen können sollen, muß die WAN-Connection Bridging unterstützen. Andernfalls können AppleTalk-Pakete nicht über die Verbindung weitergeleitet werden.

  Sollen UNIX-Clients statt mit UNIXWare mit TCP/IP auf NetWare-Server zugreifen können, muß die Pipeline ebenfalls als Bridge oder IP-Router konfiguriert sein. Andernfalls können TCP/IP-Pakete nicht über die Verbindung weitergeleitet werden.

IPX im Antwortprofil

Bevor die Pipeline einen ankommenden Ruf beantwortet, überprüft sie die Einstellungen in ihrem Antwortprofil. Enthält der Ruf nicht die vom Antwortprofil benötigten Informationen (wie Name und Kennwort), beendet die Pipeline den Ruf. Das Antwortprofil enthält die folgenden für das IPX-Routing relevanten Parameter:

Tabelle 8-2: IPX-Routing-Parameter im Antwortprofil

Ort	Parameter mit Beispielwerten
Ethernet > Answer > PPP options... (Antwortprofil)	Route IPX=Yes Recv Auth=Either
Ethernet > Answer > Sessions options...	IPX SAP Filter=1

Weitere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Hinweis: Im Gegensatz zu IP-Routing-Konfigurationen, bei denen die Pipeline das rufende Gerät eindeutig an dessen IP-Adresse erkennt, gibt es beim IPX-Routing keine „eingebaute“ Methode, die rufende Seite eindeutig bestimmen zu können. Daher muß mit Kennwort-Authentifizierung mit PAP bzw. CHAP gearbeitet werden, wenn nicht im selben Verbindungsprofil auch IP-Routing aktiviert wurde.

Zum Festlegen der Antwortprofil-Parameter, mit denen ankommende IPX-Routing-Rufe zugelassen werden, ist wie folgt vorzugehen:

1 Öffnen Sie das „Answer“-Profil.

2 Öffnen Sie das Untermenü „PPP Options“.

3 Aktivieren Sie das IPX-Routing.

```
Route IPX=Yes
```

4 Legen Sie das Authentifizierungsverfahren fest.

Beispiel:

```
Recv Auth=Either
```

Weitere Informationen zur Einrichtung der Authentifizierung finden Sie im Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Zum Zuweisen eines IPX-SAP-Filters zum Antwortprofil ist wie folgt vorzugehen:

5 Öffnen Sie das Untermenü „Session Options“.

6 Geben Sie die Nummer des von Ihnen definierten IPX-SAP-Filterprofils an.

Die IPX-SAP-Filterprofile und ihre Nummern finden Sie im Menü „IPX SAP Filters“. Geben Sie den eindeutigen Teil der Nummer (z. B. 1, 2, 3,…) an.

Beispiel:

```
IPX SAP Filter=1
```

Siehe dazu „Filter für den SAP-Verkehr“ auf Seite 8-23.

7 Schließen Sie das „Answer“-Profil.

Integrieren der Pipeline in das lokale IPX-Netzwerk

Das Verbinden der Pipeline mit Ihrem lokalen IPX-Netzwerk umfaßt die folgenden Hauptschritte:

- Aktivieren des IPX-Routing
- Festlegen des IPX-Rahmentyps für das Routing und das Watchdog-Spoofing
- Angeben der IPX-Netzwerknummer der Pipeline (bzw. die Nummer von anderen Routern lernen lassen)

Außerdem empfiehlt es sich u. U., eine IPX-Netzwerknummer für Einwähl-Clients zu definieren. In Tabelle 8-3 werden die IPX-Routing-Parameter im Ethernet-Profil aufgeführt.

Tabelle 8-3: IPX-Routing-Parameter im Ethernet-Profil

Ort	Parameter mit Beispielwerten
Ethernet > Mod Config (Ethernet-Profil)	IPX Routing=Yes
Ethernet > Mod Config > Ether options...	IPX Frame=802.2 IPX Enet #=00000000 IPX Pool #=cccc1234 IPX SAP Filter=1

Weitere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch.*

Überprüfen der lokalen NetWare-Konfigurationen

IPX-Pakete können in einem Ethernet-Segment verschiedene Ethernet-Rahmentypen haben. Routing und Watchdog-Spoofing ist jedoch nur für den IPX-Rahmentyp möglich, den Sie angegeben haben. (Wenn Bridging aktiviert wurde, werden die IPX-Pakete mit einem anderen Rahmentyp „gebridgt“.)

Zum Überprüfen der IPX-Konfiguration eines NetWare-Servers im lokalen Ethernet ist wie folgt vorzugehen:

1. Gehen Sie zur Konsole des NetWare-Servers.
2. Geben Sie „LOAD INSTALL“ ein, um die AUTOEXEC.NCF anzuzeigen.
3. Suchen Sie nach Zeilen, die so ähnlich wie die folgenden aussehen:

```
internal network 1234
Bind ipx ipx-card net=CF0123FF
Load 3c509 name=ipx-card frame=ETHERNET_8023
```

Die erste Zeile gibt die interne Netzwerknummer des Servers an. Informationen zu den internen Netzwerknummern finden Sie in Ihrer NetWare-Dokumentation. Für Ascend-Einheiten werden keine internen Netzwerknummern benötigt.

In der „BIND“-Zeile wird die im Ethernet verwendete IPX-Netzwerknummer angegeben. Die Pipeline muß für ihre Ethernet-Schnittstelle dieselbe IPX-Netzwerknummer verwenden. Sie können die Nummer entweder explizit im Ethernet-Profil der Pipeline festlegen oder aber die Pipeline-Nummer auf 0 (Null) setzen, so daß sie ihre Nummer von anderen Routern „lernt“.

In der „LOAD“-Zeile wird angegeben, welchen Paket-Rahmentyp der Ethernet-Controller des Servers verwendet (in diesem Beispiel Rahmen vom Typ 802.3). Nähere Informationen zu Paketrahmen finden Sie in Ihrer Novell-Dokumentation.

Hinweis: IPX-Netzwerknummern in jedem Netzwerksegment und internen Netzwerk innerhalb eines Servers im *gesamten WAN* müssen über eine eindeutige Netzwerknummer verfügen. Sie sollten also sowohl die gerade verwendeten externen als auch die verwendeten internen Netzwerknummern an allen Standorten kennen.

Konfigurieren von IPX im Ethernet-Profil (Ethernet-->Mod Config)

Wenn Sie IPX-Routing in der Pipeline aktivieren und das Ethernet-Profil schließen, befindet sich die Pipeline standardmäßig im IPX-Routing-Modus. Dabei wird der Standard-Rahmentyp 802.2 (der für NetWare 3.12 und höher empfohlene Rahmentyp) verwendet, und die Pipeline hört sich im Ethernet um, um von anderen IPX-Routern in diesem Ethernet-Segment ihre IPX-Netzwerknummer zu erfahren.

Aktivieren Sie das IPX-Routing in der Pipeline. Gehen Sie dazu wie folgt vor:

1 Öffnen Sie „Ethernet-->Mod Config“.

2 Aktivieren Sie das IPX-Routing.

```
IPX Routing=Yes
```

Geben Sie nun den IPX-Rahmentyp an. Gehen Sie dazu wie folgt vor:

3 Öffnen Sie das Untermenü „Ether Options“.

4 Geben Sie den IPX-Rahmentyp an („IPX Frame“).

Beispiel:

```
IPX Frame=802.2
```

Hinweis: Stellen Sie sicher, daß der von Ihnen angegebene Typ dem Rahmentyp entspricht, den die meisten Server im lokalen Netzwerk verwenden.

Konfigurieren Sie die Pipeline so, daß sie ihre IPX-Netzwerknummer erlernen kann. Gehen Sie dazu wie folgt vor:

5 Setzen Sie für den Parameter „IPX Enet #“ den Wert „0“ (Null) fest.

```
IPX Enet #=00000000
```

Mit diesem Wert wird festgelegt, daß die Pipeline ihre Netzwerknummer von einem anderen Router erlernen kann. Sie können aber auch eine andere IPX-Netzwerknummer als Null eingeben, wie zum Beispiel:

```
IPX Enet #=C90AB997
```

Hinweis: Wenn Sie eine andere IPX-Netzwerknummer als Null festlegen, wird die Pipeline zu einem „Stammrouter“, so daß andere Router ihre Nummer von der Pipeline lernen können. In diesem Fall sollten Sie sicherstellen, daß die von Ihnen eingegebene Nummer dieselbe ist, die auch von anderen IPX-Routern im selben Netzwerk verwendet wird. Nähere Informationen zum Thema Stammrouter entnehmen Sie bitte der Novell-Dokumentation.

6 Schließen Sie „Ethernet-->Mod Config“.

Um zu überprüfen, ob die Pipeline ihre IPX-Adresse gelernt hat und im Netzwerk voll verfügbar ist, können Sie am NetWare-Server den Befehl „IPXPING“ eingeben.

Überprüfen der Konfiguration mit „IPXPING“

Mit dem Befehl „IPXPING“ können Sie den Übertragungspfad zu NetWare-Stationen in der Netzwerkschicht überprüfen. Er funktioniert sowohl im selben LAN wie die Pipeline als auch über eine WAN-Verbindung, bei der IPX-Routing aktiviert ist.

Der Befehl „IPXPING“ ist im folgenden Format einzugeben:

```
ipxping <Hostname>
```

wobei <Hostname> entweder die IPX-Adresse der NetWare-Workstation oder der bekanntgemachte Name des Servers ist. Die IPX-Adresse besteht aus der IPX-Netzwerknummer und der Knotennummer für die Station, z. B.:

```
ipxping CFFF1234:000000000001
```

Wenn Sie „IPXPING“ verwenden wollen, um die Verbindung zu einem bekanntgemachten NetWare-Server zu überprüfen, können Sie einfach den Namen des Servers eingeben, z. B.:

```
ipxping server-1
```

„IPXPING“ kann durch Drücken der Tastenkombination Strg-C jederzeit abgebrochen werden.

Definieren eines virtuellen IPX-Netzwerks für Einwähl-Clients

Einwähl-Clients gehören nicht zum IPX-Netzwerk. Sie müssen daher eine IPX-Netzwerknummer zugewiesen bekommen, um eine Routing-Verbindung mit der Pipeline aufzubauen. Um Einwähl-Clients eine IPX-Netzwerknummer zuweisen zu können, müssen Sie im Ethernet-Profil („Ethernet-->Mod Config“) ein „virtuelles“ IPX-Netzwerk definieren. Die Pipeline macht die Route zu diesem virtuellen Netzwerk bekannt und weist sie als Netzwerkadresse für Einwähl-Clients zu. Siehe dazu „Definieren eines virtuellen IPX-Netzwerks für Einwähl-Clients“ auf Seite 8-15.

Hinweis: Der häufigste Konfigurationsfehler bei NetWare-Verbindungen zwischen zwei Netzwerken ist die Zuweisung doppelter Netzwerknummern. Achten Sie daher darauf, daß die Netzwerknummer, die Sie im Parameter „IPX Pool#“ angeben, nicht bereits innerhalb der gesamten IPX-Routing-Domäne der Pipeline vergeben ist.

Konfigurieren Sie die Pipeline mit einem virtuellen IPX-Netzwerk für Einwähl-Clients. Gehen Sie dazu wie folgt vor:

1 Öffnen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

2 Öffnen Sie das Untermenü „Ether Options“.

3 Legen Sie im Parameter „IPX Pool #“ eine 32 Bit große hexadezimale IPX-Netzwerknummer fest, die bisher in der gesamten IPX-Routing-Domäne noch nicht vergeben ist.

Beispiel:

```
IPX Pool #=cccc1234
```

4 Schließen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

Verwalten der RIP- und SAP-Tabellen

In Zusammenhang mit RIP- und SAP-Tabellen können Sie die folgenden Verwaltungsaufgaben durchführen:

- Anzeigen der RIP- und SAP-Tabellen
- Konfigurieren von RIP in Verbindungsprofilen
- Konfigurieren einer statischen Route
- Konfigurieren von SAP in Verbindungsprofilen
- Definieren und Anwenden von IPX-SAP-Filtern

Darüber hinaus können auch Standard-Ruffilter oder -Datenfilter definiert werden, um ein größeres Maß an Kontrolle über den WAN-Verkehr und die WAN-Verbindungen zu erhalten. Weitere Informationen zum Thema Filter finden Sie in Kapitel 10, „Definieren von Filtern“.

Anzeigen der RIP- und SAP-Tabellen

Wenn Sie sich die aktuelle RIP-Tabelle anzeigen lassen wollen, rufen Sie die Terminal-Server-Schnittstelle auf, und geben Sie in der Befehlszeile den folgenden Befehl ein:

```
ascend% show netware networks
```

Auf dem Bildschirm erscheint die folgende Anzeige (angegebene Werte sind Beispielwerte):

```
network       next router         hops     ticks     origin
22222222      000000000000        2        12        nov12-m2        S
A30E0A04      0080A30E0A04        1        3         Ethernet
A30E1347      0080A30E1347        1        3         Ethernet
A30E0EB8      0080A30E0EB8        1        3         Ethernet
A304B294      0080A304B294        1        3         Ethernet
EE000001      00608CB24081        1        3         Ethernet
AA000002      000000000000        0        1         Ethernet        S
```

Die RIP-Tabelle enthält die folgenden Felder:

- „Network“ zeigt die interne Netzwerknummer eines NetWare-Servers an.
- „Next Router“ ist die Adresse eines IPX-Routers, der zur Weiterleitung der Pakete zu diesem Server verwendet wird.
- „Hops“ zeigt den Hop-Wert für die Strecke zum Zielnetzwerk (Server) an.
- „Ticks“ (in 1/18 Sekunden) zeigt den Tick-Wert für die Strecke zum Zielnetzwerk (Server) an.

  Die beste Route wird auf der Grundlage des Tick-Wertes, nicht auf der des Hop-Wertes berechnet.
- „Origin“ zeigt an, welches Verbindungsprofil verwendet werden soll, um den Server zu erreichen.

Damit die aktuelle IPX-SAP-Tabelle angezeigt wird, ist an der Terminal-Server-Eingabeaufforderung der folgende Befehl einzugeben:

```
ascend% show NetWare-Server
```

Auf dem Bildschirm erscheint die folgende Anzeige (angegebene Werte sind Beispielwerte):

```
       IPX address                    type         server name
EE000001:000000000001:0040            026b       ASCEND__________
EE000001:000000000001:4510            0004       NOVL1
EE000001:000000000001:4005            0278       ASCEND__________
A30E0A04:000000000001:8060            0047       EPS_0E0A04
A30E1347:000000000001:8060            0047       EPS_0E1347
A30E0EB8:000000000001:8060            0047       EPS_0E0EB8
A30EB294:000000000001:8060            0047       EPS_04B294
```

Die SAP-Tabelle enthält die folgenden Felder:

- „IPX Address“ zeigt die IPX-Adresse eines Servers an.
  Dabei wird folgendes Format verwendet:
  <Netzwerknummer>:<Knotennummer>:<Socket-Nummer>
- „Type“ zeigt die hexadezimale Nummer eines NetWare-Diensttyps an.
  Zum Beispiel lautet die Nummer für Dateidienste 0004.
- „Server Name“ zeigt den Namen des Servers an (max. 35 Zeichen).

Einschränken des RIP-Austausches in Verbindungsprofilen

Der Parameter „IPX RIP“ ist in Verbindungsprofilen standardmäßig auf „Both“ gesetzt, so daß RIP-Broadcasts in beide Richtungen ausgetauscht werden. Sie haben jedoch die Möglichkeit, den Austausch von RIP-Broadcasts über eine WAN-Verbindung zu deaktivieren oder festzulegen, daß die Pipeline RIP-Broadcasts über die jeweilige Verbindung nur sendet bzw. nur empfängt. Wenn die Pipeline keine RIP-Broadcasts von einer entfernten Einheit empfängt, sollten Sie eine statische Route zu mindestens einem Server in diesem Netzwerk konfigurieren (siehe dazu den nächsten Abschnitt).

Wenn Sie den Austausch von RIP-Broadcasts über eine WAN-Verbindung einschränken wollen, gehen Sie wie folgt vor:

1 Öffnen Sie ein „Connections“-Profil, bei dem IPX-Routing aktiviert ist.

2 Öffnen Sie das Untermenü „IPX Options“.

3 Legen Sie für den Parameter „IPX RIP“ einen anderen Wert als den Standardwert „Both“ fest.

Beispiel:

```
IPX RIP=Recv
```

Bei dieser Einstellung empfängt die Pipeline die RIP-Tabelle vom anderen IPX-Router, gibt aber ihre RIP-Tabelle nicht weiter. Soll „IPX RIP“ ganz deaktiviert werden, ist folgender Wert festzulegen:

```
IPX RIP=None
```

4 Schließen Sie das „Connections“-Profil.

Konfigurieren einer statischen IPX-Route

Jede statische IPX-Route enthält alle Informationen, die benötigt werden, um einen NetWare-Server in einem entfernten Netzwerk zu erreichen. Wenn die Pipeline ein abgehendes Paket für diesen Server empfängt, sucht sie nach dem angegebenen Verbindungsprofil und wählt die Verbindung.

Tabelle 8-4 zeigt die IPX-Routing-Profil-Parameter:

Tabelle 8-4: IPX-Routing-Profil-Parameter

Ort	Parameter mit Beispielwerten
Ethernet > IPX-Routen > *alle Profile* (IPX-Routing-Profil)	Server Name=SERVER-1 Active=Yes Network=ccccfff1 Node=000000000001 Socket=0000 Server Type=0004 Hop Count=2 Tick Count=12 Connection #=1

Weitere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Hinweis: Für Server innerhalb des lokalen Ethernet-Netzwerks müssen keine IPX-Routen erstellt werden.

An den meisten Standorten werden nur einige wenige IPX-Routen angelegt. Für die meisten anderen Verbindungen wird RIP verwendet. Wenn sich auf beiden Seiten der WAN-Verbindung Server befinden, empfiehlt es sich, eine statische Route zum entfernten Standort zu definieren, selbst wenn für Ihre Umgebung dynamische Routen benötigt werden. Haben Sie eine statische Route zu einem entfernten Standort, sollte in ihr ein „Master"-NetWare-Server angegeben sein, der viele andere Dienste kennt. Über eine Verbindung zu diesem Server können dann die NetWare-Workstations über andere entfernte Dienste informiert werden.

Hinweis: Beachten Sie, daß statische IPX-Routen manuell verwaltet werden. Daher müssen sie aktualisiert werden, sobald es beim entfernten Server Änderungen gibt.

Definieren Sie ein IPX-Routing-Profil. Gehen Sie dazu wie folgt vor:

1 Öffnen Sie das Menü „IPX Routes".

2 Öffnen Sie ein IPX-Routing-Profil.

3 Geben Sie den Namen des entfernten NetWare-Servers an.
Beispiel:
`Server Name=SERVER-1`

4 Geben Sie an, daß die Route in die RIP-Tabelle aufgenommen werden soll.
`Active-Yes`

5 Geben Sie die interne Netzwerknummer des entfernten Servers an.
Beispiel:
`Network=ABC01FFF`

6 Geben Sie die Knotennummer des entfernten Servers an.
Beispiel:
`Node=0000000000001`
Der Standardwert „0000000000001" ist im Normalfall die Knotennummer für NetWare-File-Server.

7 Geben Sie die Socket-Nummer des entfernten Servers an.
Beispiel:
`Socket=0451`
Novell-File-Server verwenden meistens die Socket-Nummer 0451.
Die von Ihnen angegebene Socket-Nummer muß eine allgemein bekannte Nummer sein. Dienste, die dynamische Socket-Nummern benutzen,

verwenden u. U. bei jedem Laden eine andere Socket und arbeiten nicht mit IPX-Routing-Profilen. Um eine Verbindung zu einem entfernten Dienst aufzubauen, die eine dynamische Socket-Nummer verwendet, ist ein „Master"-Server im gleichen Netzwerk anzugeben, der eine allgemein bekannte Socket-Nummer verwendet.

8 Geben Sie den Typ des SAP-Dienstes an.

Beispiel:

```
Service Type=0004
```

NetWare-File-Server haben den SAP-Diensttyp 0004.

9 Geben Sie die Entfernung zum Server (in Hops) an.

Beispiel:

```
Hop count=2
```

Im Normalfall ist der Standardwert 2 angemessen.

10 Geben Sie die Entfernung zum Server in Ticks (1/18 Sekunde) an.

Beispiel:

```
Tick count=12
```

Im Normalfall ist der Standardwert 12 angemessen, aber u. U. macht es sich erforderlich, diesen Wert für weiter entfernte Server zu erhöhen.

11 Geben Sie die Nummer des Verbindungsprofils für die WAN-Verbindung an.

Zur Angabe der Nummer des Verbindungsprofils ist der eindeutige Teil der jeweiligen Nummer im Menü „Connections" zu verwenden (1, 2, 3 usw.).

```
Connection #=2
```

12 Schließen Sie das IPX-Routing-Profil.

Einschränken des SAP-Austausches in Verbindungsprofilen

Der Parameter „IPX SAP" ist in „Connections"-Profilen standardmäßig auf „Both" gesetzt, so daß RIP-Broadcasts in beide Richtungen ausgetauscht werden. Wenn die Pipeline so konfiguriert ist, daß SAP-Broadcasts über die WAN-Schnittstelle sowohl gesendet als auch empfangen werden können, sendet die Pipeline ihre SAP-Tabelle an das entfernte Netzwerk und empfängt von diesem Netzwerk gesendete SAP-Tabellen-Aktualisierungen, so daß letztendlich beide Netzwerke über eine vollständige Tabelle aller Dienste im WAN verfügen.

Sie haben die Möglichkeit festzulegen, welche Dienste wo angeboten werden. Dazu können Sie den Austauch von SAP-Broadcasts über eine WAN-Verbindung ganz unterbinden oder aber festlegen, daß die Pipeline SAP-Broadcasts über diese Verbindung entweder nur sendet oder nur empfängt.

Wenn Sie den Austausch von SAP-Broadcasts über eine WAN-Verbindung einschränken wollen, gehen Sie wie folgt vor:

1. Öffnen Sie ein „Connections“-Profil, bei dem IPX-Routing aktiviert ist.
2. Öffnen Sie das Untermenü „IPX Options“.
3. Legen Sie für den Parameter „IPX SAP“ einen anderen Wert als den Standardwert „Both“ fest.

   Beispiel:

   ```
   IPX SAP=Recv
   ```

   Bei dieser Einstellung empfängt die Pipeline SAP-Tabellen-Aktualisierungen vom entfernten Router. Wenn Sie nicht wollen, daß die Pipeline SAP-Broadcasts über diese Verbindung sendet oder empfängt, muß für „IPX SAP“ folgendes festgelegt werden:

   ```
   IPX SAP=None
   ```
4. Schließen Sie das „Connections“-Profil.

Filter für den SAP-Verkehr

Mit Hilfe von IPX-SAP-Filtern können bestimmte NetWare-Dienste in die SAP-Tabelle der Pipeline aufgenommen oder aus ihr ausgeschlossen werden.

Hinweis: IPX-SAP-Filter dienen zur Festlegung, welche Dienste der lokalen SAP-Tabelle hinzugefügt oder in SAP-Antwortpaketen über IPX-Routing-Verbindungen (*nicht* IPX-Bridging-Verbindungen) weitergeleitet werden sollen. Sie können nicht zur Einsparung von Verbindungsgebühren verwendet werden, wie das bei Filtern der Fall ist, die verhindern, daß regelmäßige RIP- und SAP-Broadcasts eine Verbindung unnötig aufrechterhalten.

In Tabelle 8-5 sind die Parameter für IPX-SAP-Filter aufgeführt:

Tabelle 8-5: IPX-SAP-Filterprofil-Parameter

Ort	**Parameter mit Beispielwerten**
Ethernet > IPX-SAP-Filter > *alle Profile* (IPX-SAP-Filterprofil)	Name=optional Input filters... Output filters... Valid=Yes Type=Exclude Server Type=0004 Server Name=SERVER-5
Ethernet > Connections > *alle Profile* > Sessions options… (Verbindungsprofil)	IPX SAP Filter=1
Ethernet > Mod Config > Ether options… (Ethernet-Profil).	IIPX SAP Filter=1
Ethernet > Answer > Sessions options... (Antwortprofil)	IPX SAP Filter=1

Weitere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Definieren eines IPX-SAP-Filters

Zum Definieren eines IPX-SAP-Filters (Filterprofil) ist wie folgt vorzugehen:

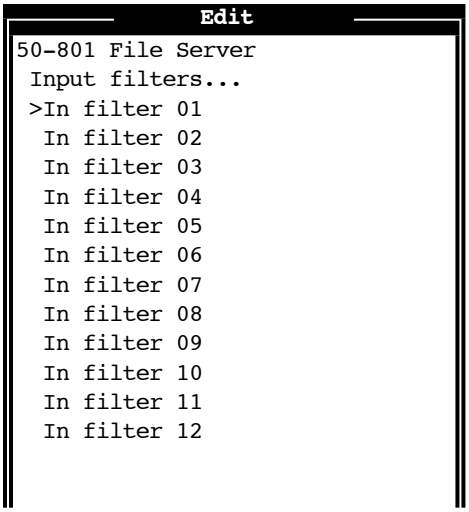
1 Öffnen Sie das Menü „IPX SAP Filters“, und öffnen Sie dann ein Profil.

2 Geben Sie einen Namen für das Profil an.

3 Öffnen Sie die Liste der Eingangsfilter („Input Filters“).

Eingangsfilter gelten für alle von der Pipeline empfangenen SAP-Pakete. Sie suchen nach bekanntgemachten Diensten und schließen diese entsprechend den Filterkriterien aus der SAP-Tabelle der Pipeline aus bzw. nehmen sie in die Tabelle auf.

Sie können maximal 12 Filter festlegen, um 12 Diensttypen bzw. Dienste aus der Tabelle auszuschließen bzw. in diese aufzunehmen. Diese Filter werden in der Reihenfolge abgearbeitet, in der sie aufgeführt sind, d. h. zuerst „In filter 01“, dann „In filter 02“ usw.



4 Öffnen Sie das Menü zur Festlegung der Kriterien für den ersten Filter, indem Sie „In filter 01“ markieren und die Eingabetaste drücken.

5 Legen Sie für den Parameter „Valid“ den Wert „Yes“ fest.

```
Valid=Yes
```

6 Legen Sie für den Filtertyp (Parameter „Type“) den Wert „Exclude“ fest.

```
Type=Exclude
```

7 Geben Sie den Diensttyp an (hexadezimale Zahl).

Beispiel:

```
Server Type=4
```

File-Server haben den Diensttyp 4.

8 Geben Sie den Namen des NetWare-Servers an (in diesem Beispiel „SERVER-1“).

```
Edit
50-801 File Server
 In filter 01
 >Valid=Yes
  Type=Exclude
  Server Type=4
  Server Name=SERVER-1
```

9 Schließen Sie „In filter 01“.

10 Legen Sie, falls erforderlich, die Werte für weitere Eingangsfilter fest.

11 Drücken Sie so oft die Esc-Taste, bis Sie zur obersten Ebene des Profils zurückgekehrt sind.

12 Öffnen Sie die Liste der Ausgabefilter („Output filters“).

Ausgabefilter werden auf SAP-Antwortpakete angewendet, die von der Pipeline gesendet werden. Wenn die Pipeline ein SAP-Anforderungspaket empfängt, wendet sie vor dem Versenden der Antwort auf das SAP-Antwortpaket einen Filter an, um den Dienst entsprechend den festgelegten Filterkriterien aus dem Antwortpaket aus- bzw. in dieses einzuschließen.

Sie können maximal 12 Filter festlegen, um 12 Diensttypen bzw. Dienste aus den Antwortpaketen auszuschließen bzw. in diese aufzunehmen. Diese Filter werden in der Reihenfolge abgearbeitet, in der sie aufgeführt sind, d. h. zuerst „Out filter 01“, dann „Out filter 02“ usw.

Definieren Sie die Filterkriterien.

13 Schließen Sie das IPX-SAP-Filterprofil.

Anwenden von IPX-SAP-Filtern

Sie können IPX-SAP-Filter entweder auf die lokale Ethernet-Schnittstelle oder auf die WAN-Schnittstellen oder auf beide Schnittstellenarten anwenden.

- Im Ethernet-Profil können mit einem SAP-Filter bestimmte Server oder Dienste aus der Tabelle ausgeschlossen oder in diese aufgenommen werden.

  Wenn keine Verzeichnisdienste unterstützt werden, sind Server oder Dienste, die nicht in der Pipeline-Tabelle verzeichnet sind, für Clients über das WAN nicht erreichbar.
- Im „Answer“-Profil dient der SAP-Filter zur Überwachung von Dienstbekanntmachungen über das WAN.
- In „Connections“-Profilen dient der SAP-Filter zur Überwachung von Dienstbekanntmachungen von und zu einer spezifischen WAN-Verbindung.

Um einen IPX-SAP-Filter auf SAP-Pakete anzuwenden, ist wie folgt vorzugehen:

1 Öffnen Sie das IPX-SAP-Filterprofil.

2 Öffnen Sie das Untermenü „Session Options“ („Answer“- und „Connections“-Profil) bzw. das Untermenü „Ether Options“ (Ethernet-Profil).

3 Geben Sie die Nummer des von Ihnen definierten IPX-SAP-Filterprofils an.

Zur Zuweisung eines IPX-SAP-Filterprofils müssen Sie den eindeutigen Teil der Nummer des Profils im Menü „IPX SAP Filters“ angeben. So ist z. B. für die Zuweisung des Filters „20-801“ folgendes einzugeben:

```
IPX SAP Filter=1
```

4 Schließen Sie das Profil.

Filter, die der Ethernet-Schnittstelle zugewiesen werden, sind sofort wirksam.

Konfigurieren von IPX-Routing-Verbindungen

In diesem Abschnitt wird die Konfiguration von IPX-Routing-Verbindungen beschrieben. Neben einer Beschreibung der Voraussetzungen für die Host-Software finden Sie hier auch verschiedene Beispielkonfigurationen:

- Beispiel für eine Einwähl-Client-Verbindung
- Beispiel mit einem Server auf beiden Seiten der Verbindung
- Beispiel mit einem Server auf nur einer Seite der Verbindung

In Tabelle 8-6 sind die Verbindungsprofil-Parameter für das IPX-Routing aufgeführt.

Tabelle 8-6: Parameter zur Festlegung von IPX-Routing-Verbindungen

Ort	**Parameter mit Beispielwerten**
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Station=*Gerätename* Route IPX=Yes
Ethernet > Connections > *alle Profile* > Encaps options...	Recv PW=*SECURE* Send PW=*SECURE* Send Auth=CHAP
Ethernet > Connections > *alle Profile* > IPX options...	Peer=Router Dial Query=No IPX Net#=cfff0003 IPX Alias#=00000000 Handle IPX=None Netware t/o=30
Ethernet > Connections > *alle Profile* > Sessions options…	IPX SAP Filter=1

Weitere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Beispiel für eine Einwähl-Client-Verbindung

In diesem Beispiel wählt sich ein NetWare-Client in ein IPX-Unternehmensnetzwerk ein, das sowohl Server als auch Clients unterstützt, die PPP-Einwähl-Software verwenden (siehe Abbildung 8-1).

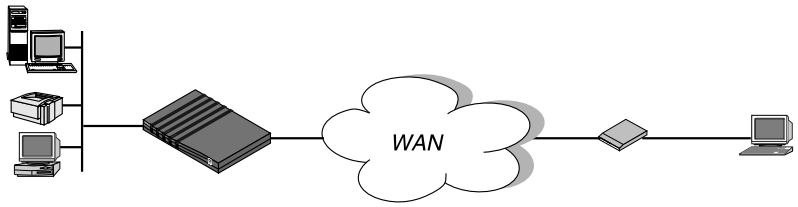


Abbildung 8-1: Einwähl-NetWare-Client, für den dynamisch eine IPX-Netzwerknummer festgelegt werden muß

In diesem Beispiel ist die Pipeline mit einem NetWare-Unternehmens-LAN verbunden, und der Einwähl-Client hat ein Modem, NetWare-Client-Software und PPP-Einwähl-Software. Bei diesem Beispiel wird davon ausgegangen, daß sowohl im Antwortprofil als auch im Ethernet-Profil IPX-Routing aktiviert ist.

Konfigurieren Sie die Pipeline so, daß sie Verbindungen vom PC des sich einwählenden Benutzers am Standort B akzeptiert. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie das Ethernet-Profil („Ethnet-->Mod Config“).
2. Weisen Sie dem Einwähl-Client eine IPX-Nummer zu.
   Beispiel:
   ```
   IPX Pool#=B21CC345
   ```
   Hinweis: Achten Sie darauf, daß diese Nummer in der gesamten IPX-Routing-Domäne nur einmal vergeben werden darf.
3. Schließen Sie das Ethernet-Profil („Ethnet-->Mod Config“).
4. Öffnen Sie das „Connections“-Profil für den Einwähl-Client.
5. Nehmen Sie die folgenden Einstellungen vor:
   ```
   Station=NetWareClient1
   Active=Yes
   ```

```
Encaps=PPP
Route IPX=Yes

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    Peer=Dialin
```

6 Schließen Sie das „Connections“-Profil.

Beispiel mit NetWare-Servern auf beiden Seiten der Verbindung

In diesem Beispiel ist die Pipeline mit einem IPX-Netzwerk verbunden, das sowohl Server als auch Clients unterstützt. Das entfernte Netzwerk unterstützt ebenfalls sowohl Server und Clients.

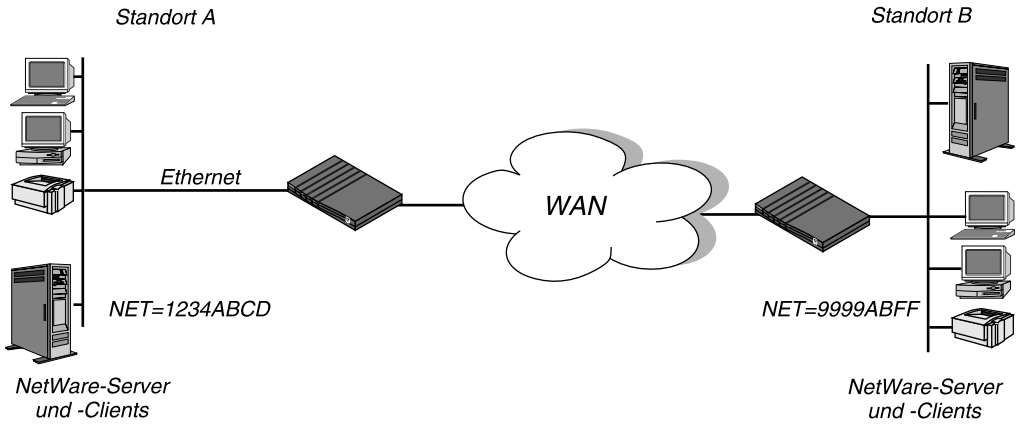


Abbildung 8-2: Verbindung mit NetWare-Servern auf beiden Seiten

In diesem Beispiel sind die beiden Netzwerke an Standort A und Standort B bestehende Novell-LANs, die NetWare-3.12- und NetWare-4-Server, NetWare-Clients und eine Pipeline unterstützen. Für den NetWare-Server am Standort A wurden die folgenden Einstellungen festgelegt:

```
Name=SERVER-1
internal net CFC12345
Load 3c509 name=ipx-card frame=ETHERNET_8023
Bind ipx ipx-card net=1234ABCD
```

Der NetWare-Server am Standort B ist folgendermaßen konfiguriert:

```
Name=SERVER-2
internal net 013DE888
Load 3c509 name=net-card frame=ETHERNET_8023
Bind ipx net-card net=9999ABFF
```

Konfigurieren Sie die Pipeline am Standort A:

1 Weisen Sie der Pipeline, falls noch nicht geschehen, mit Hilfe des Parameters „Name“ im Systemprofil einen Namen zu.

Beispiel:

```
Name=PIPELAGW
```

2 Öffnen Sie das „Connections“-Profil für Standort B.

In diesem Beispiel ist das „Connections“-Profil für Standort B das Profil #5.

Legen Sie die Einstellungen für das „Connections“-Profil fest:

```
Station=PIPELBGW
Active=Yes
Encaps=MPP
Dial #=555-1212
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=None
    IPX SAP=Both
    NetWare t/o=30
```

3 Schließen Sie das „Connections“-Profil #5.

4 Öffnen Sie das Ethernet-Profil („Ethnet-->Mod Config“), und aktivieren Sie, falls noch nicht geschehen, das IPX-Routing.

Beispiel:

```
IPX Routing=Yes

Ether options...
    IPX Frame=802.2
    IPX Enet #=1234ABCD
```

5 Schließen Sie das Ethernet-Profil („Ethnet-->Mod Config“).

Da für „IPX RIP“ im „Connections“-Profil der Wert „None“ festgelegt wurde, muß eine statische Route zum entfernten Server konfiguriert werden:

6 Öffnen Sie ein IPX-Routing-Profil.

7 Richten Sie eine Route zum entfernten NetWare-Server ein. Verwenden Sie dazu die folgenden Einstellungen:

```
Server Name=SERVER-2
Active=Yes
Network=013DE888
Node=000000000001
Socket=0451
Server Type=0004
Connection #=5
```

Hinweis: Der Wert des Parameters „Connection #“ im IPX-Routing-Profil muß mit der für diesen Standort konfigurierten Nummer im Verbindungsprofil übereinstimmen.

8 Schließen Sie das IPX-Routing-Profil.

Die Pipeline am Standort B ist wie folgt zu konfigurieren:

Weisen Sie der Pipeline, falls noch nicht geschehen, mit Hilfe des Parameters „Name“ im Systemprofil einen Namen zu.

Beispiel:

```
Name=PIPELBGW
```

9 Öffnen Sie das „Connections“-Profil für Standort A.

In diesem Beispiel ist das Verbindungsprofil für Standort A das Profil #2.

Richten Sie das Verbindungsprofil wie folgt ein:

```
Station=PIPELAGW
Active=Yes
Encaps=MPP
Dial #=555-1213
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=None
    IPX SAP=Both
    NetWare t/o=30
```

10 Schließen Sie das „Connections“-Profil #2.

11 Öffnen Sie das Ethernet-Profil („Ethnet-->Mod Config“), und aktivieren Sie, falls noch nicht geschehen, das IPX-Routing.

Beispiel:

```
IPX Routing=Yes

Ether options...
    IPX Frame=802.2
    IPX Enet #=9999ABFF
```

12 Schließen Sie das Ethernet-Profil („Ethnet-->Mod Config“).

Da für „IPX RIP“ im „Connections“-Profil der Wert „None“ festgelegt wurde, muß eine statische Route zum entfernten Server konfiguriert werden:

13 Öffnen Sie ein IPX-Routing-Profil.

14 Richten Sie eine Route zum entfernten NetWare-Server ein. Verwenden Sie dazu die folgenden Einstellungen:

```
Server Name=SERVER-1
Active=Yes
Network=CFC12345
Node=000000000001
Socket=0451
Server Type=0004
Connection #=2
```

Hinweis: Der Wert des Parameters „Connection #“ im IPX-Routing-Profil muß mit der für diesen Standort konfigurierten Nummer im „Connections“-Profil übereinstimmen.

15 Schließen Sie das IPX-Routing-Profil.

Beispiel mit NetWare-Servern nur im lokalen Netzwerk

In diesem Beispiel ist die Pipeline mit einem lokalen IPX-Netzwerk verbunden, das sowohl Server als auch Clients unterstützt. Es soll eine Verbindung zu einem entfernten Netzwerk aufgebaut werden, das einen oder mehrere NetWare-Clients (aber keine Server) unterstützt (siehe Abbildung 8-3).

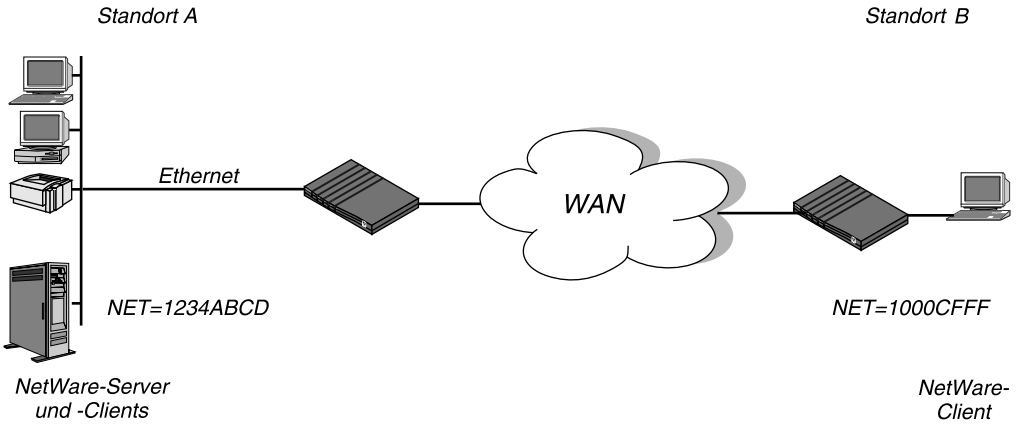


Abbildung 8-3: Einwähl-Client, der in sein eigenes IPX-Netzwerk eingebunden ist

In diesem Beispiel unterstützt Standort A NetWare-3.12 Server, NetWare-Clients und eine Pipeline. Der NetWare-Server am Standort A ist wie folgt konfiguriert:

```
Name=SERVER-1
internal net CFC12345
Load 3c509 name=ipx-card frame=ETHERNET_8023
Bind ipx ipx-card net=1234ABCD
```

Standort B ist ein Heimbüro, das aus einem PC und einer Ascend-Einheit besteht. Dabei handelt es sich nicht um ein bestehendes Novell-LAN, so daß die Ascend-Einheit so konfiguriert ist, daß ein neues IPX-Netzwerk angelegt wird (z. B. „1000CFFF“).

Hinweis: Die dem Standort B in diesem Beispiel zugewiesene neue IPX-Netzwerknummer darf innerhalb des gesamten IPX-WANs (weder am Standort A noch in einem der Netzwerke, mit denen der Standort A verbunden ist) nicht bereits verwendet werden.

In diesem Beispiel wird davon ausgegangen, daß IPX-Routing sowohl im Ethernet-Profil („Ethnet-->Mod Config“) als auch im „Answer“-Profil bereits aktiviert wurde. Da keine statischen Routen verwendet werden, sollte die erste Verbindung zwischen den beiden Ascend-Einheiten mit Hilfe des DO-Menüs manuell gewählt werden.

Zum Konfigurieren der Pipeline am Standort A ist wie folgt vorzugehen:

1 Weisen Sie der Pipeline, falls noch nicht geschehen, mit Hilfe des Parameters „Name“ im Systemprofil einen Namen zu.

Beispiel:

```
Name=PIPELAGW
```

2 Öffnen Sie das „Connections“-Profil für Standort B.

Legen Sie die Einstellungen für das „Connections“-Profil fest:

```
Station=PIPELBGW
Active=Yes
Encaps=MPP
Dial #=555-1212
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A
```

```
Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=Both
    IPX SAP=Both
    NetWare t/o=30
```

3 Schließen Sie das „Connections“-Profil.

Die Ascend-Einheit am Standort B ist wie folgt zu konfigurieren:

1 Weisen Sie der Ascend-Einheit, falls noch nicht geschehen, mit Hilfe des Parameters „Name“ im Systemprofil einen Namen zu.

Beispiel:

```
Name=PIPELBGW
```

2 Öffnen Sie das „Connections“-Profil für Standort A.

Legen Sie die Einstellungen für das „Connections“-Profil fest:

```
Station=PIPELAGW
Active=Yes
Encaps=MPP
Dial #=555-1213
Route IP=No
Route IPX=Yes
Bridge=No
Dial brdcast=N/A

Encaps options...
    Send Auth=CHAP
    Recv PW=*SECURE*
    Send PW=*SECURE*

IPX options...
    IPX RIP=Both
    IPX SAP=Both
    NetWare t/o=30
```

3 Schließen Sie das „Connections“-Profil, und speichern Sie die Änderungen.

Einrichten der Pipeline-Sicherheit

9

Dieses Kapitel enthält die folgenden Abschnitte:

Empfohlene Sicherheitsmaßnahmen

Bei der Lieferung der Pipeline ab Werk sind die Sicherheitsfunktionen alle auf Standardwerte gesetzt, mit denen Sie die Pipeline ohne jede Zugangsbeschränkung konfigurieren und einrichten können. Bevor Sie die Pipeline allgemein zugänglich machen, sollten diese Standard-Sicherheitseinstellungen geändert werden, um zu verhindern, daß Unbefugte auf die konfigurierte Einheit zugreifen können.

Bevor die Pipeline zugänglich gemacht wird, empfiehlt es sich, die folgenden Sicherheitsmaßnahmen vorzunehmen:

- Ändern des Kennworts für die Sicherheitsstufe „Full Access“

  Benutzer, die das Kennwort für die Sicherheitsstufe „Full Access“ kennen, sind in der Lage, sämtliche Operationen mit der Pipeline auszuführen. Dazu gehört auch das Ändern der Konfigurationseinstellungen. Das „Full Access“-Kennwort lautet standardmäßig „Ascend“. Es empfiehlt sich, statt dessen ein eigenes Kennwort festzulegen.

- Aktivieren der Sicherheitsstufe „Full Access“

  Nachdem Sie Ihr Kennwort eingegeben haben, sollten Sie für sich selbst die Sicherheitsstufe „Full Access“ aktivieren, um die übrigen der hier beschriebenen grundlegenden Sicherheitsmaßnahmen auszuführen. Wenn Sie den nächsten Schritt ausgeführt haben, mit dem Sie die Standard-Sicherheitsstufe einschränken, wendet die Pipeline sofort die Einschränkungen an, wenn die Standard-Sicherheitsstufe noch aktiv ist.

- Festlegen eines Höchstmaßes an Sicherheit für die Standard-Sicherheitsstufe

  Der Zugriff auf die Pipeline-Terminal-Dienste erfolgt über Telnet. Für jeden Benutzer, der eine Telnet-Verbindung zur Einheit herstellt, gilt die Standard-Sicherheitsstufe, die in der Werkseinstellung keinerlei Einschränkungen aufweist. Im Sicherheitsprofil „Default“ sollten daher alle Zugangsprivilegien deaktiviert werden.

- Ändern der SNMP-Community-Namen

  Die Pipeline unterstützt SNMP-Traps. Damit können einer SNMP-Management-Station Alarme gesendet, Rufdetails mitgeteilt und andere Management-Informationen übermittelt werden, ohne daß diese extra abgefragt werden müssen. Die Standard-Community-Namen der Pipeline für den Lese- und Schreibzugriff sollten geändert werden, um Unbefugten den Zugang zur Pipeline über eine SNMP-Management-Station zu verwehren.

- Zuweisen eines Telnet-Kennworts

  Solange kein Telnet-Kennwort zugewiesen wurde, kann jeder lokale Benutzer, der die IP-Adresse der Pipeline kennt, eine Telnet-Verbindung mit ihr aufbauen. Wurde ein Kennwort festgelegt, muß von allen ankommenden Telnet-Sitzungen (sowohl vom lokalen Netzwerk aus als auch über das WAN) dieses Kennwort angegeben werden.

- Festlegen, daß für ankommende Verbindungen ein Profil vorhanden sein muß

  Die Verbindungen, die mit Hilfe des Antwortprofils der Pipeline aufgebaut werden, verfügen über keinerlei Sicherung (es wird weder ein Name noch ein Kennwort benötigt). Solche ungesicherten Verbindungen werden zwar von einigen Standorten zugelassen, in der Mehrzahl der Fälle ist dies jedoch nicht der Fall. Es empfiehlt sich, die Pipeline so zu konfigurieren, daß ankommende Verbindungen nur dann angenommen werden, wenn es ein entsprechend konfiguriertes Profil gibt.

- Deaktivieren von ICMP-Redirect-Paketen

  Zur Sicherung der IP-Routen der Pipeline empfiehlt es sich, die Einheit so zu konfigurieren, daß sie ICMP (Internet Control Message Protocol)-Redirect-Pakete ignoriert.

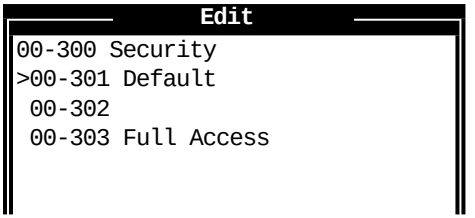
Ändern des „Full Access“-Kennworts

Das Sicherheitsprofil „Full Access“ ermöglicht Ihnen den unbeschränkten Zugang zur Pipeline. Mit diesem „Superuser“-Profil können Sie Konfigurationen ändern, entfernte Standorte anwählen, die Einheit zurücksetzen, die Systemsoftware aktualisieren usw.

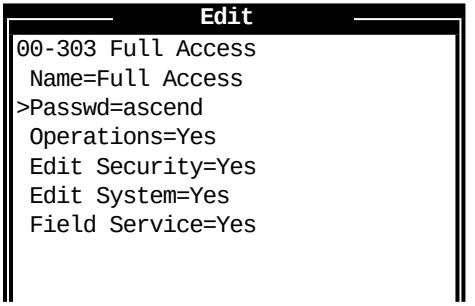
Hinweis: Wir empfehlen Ihnen, sich das „Full Access“-Kennwort aufzuschreiben und es an einem sehr sicheren Ort aufzubewahren. Außerdem sollten Sie beim Öffnen des Profils „Full Access“ darauf achten, daß das Privileg „Edit Security“ nicht deaktiviert wird, da es sonst nicht möglich ist, Privilegien zu bearbeiten, wenn „Full Access“ aktiviert ist.

Zum Ändern des „Full Access“-Kennworts ist wie folgt vorzugehen:

1 Öffnen Sie das Menü „Security“ im Menü „System“.



2 Öffnen Sie das Profil „Full Access“.



3 Geben Sie mit Hilfe des Parameters „Passwd“ ein neues Kennwort an. Drücken Sie dann die Eingabetaste.

Beispiel:

```
Passwd=mein_Kennwort
```

Hinweis: Bei der Verwendung von Kennwörtern in Ascend-Einheiten spielt die Groß- oder Kleinschreibung keine Rolle. Das Kennwort „mein_Kennwort“ kann genauso gut auch als „mein_kennwort“ oder „MEIN_KENNWORT“ eingegeben werden.

4 Lassen Sie alle anderen Privilegien aktiviert.

Hinweis: Denken Sie daran, daß das Privileg „Edit Security“ in diesem Profil nicht deaktiviert werden darf!

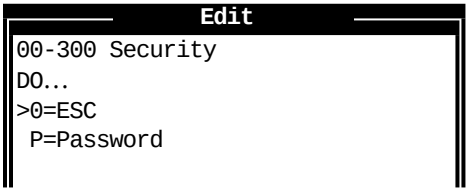
5 Schließen Sie das Profil „Full Access“.

Von jetzt an kann die Sicherheitsstufe „Full Access“ nur von Benutzern aktiviert werden, die das von Ihnen vergebene Kennwort kennen.

Aktivieren der Sicherheitsstufe „Full Access“

Um das Sicherheitsprofil „Full Access“ zu aktivieren, sind die folgenden Schritte auszuführen:

1 Drücken Sie die Tastenkombination Strg-D, um das DO-Menü zu öffnen, und drücken Sie dann die Taste P (oder wählen Sie „P=Password“).



2 Wählen Sie aus der sich daraufhin öffnenden Liste der Sicherheitsprofile den Eintrag „Full Access“.

Sie werden zur Eingabe des Kennworts aufgefordert.

3 Geben Sie das von Ihnen im Profil „Full Access“ festgelegte Kennwort ein, und drücken Sie die Eingabetaste.

Wurde das richtige Kennwort eingegeben, erscheint eine Meldung, die besagt, daß das Kennwort akzeptiert wurde und die Pipeline nun die neue Sicherheitsstufe verwendet. Bei Eingabe eines falschen Kennworts werden Sie erneut aufgefordert, das richtige Kennwort anzugeben.

Festlegen von Einschränkungen für das Sicherheitsprofil „Default“

Die Sicherheitsstufe „Default“ gilt für alle Benutzer, die eine Telnet-Verbindung zur Pipeline aufbauen oder auf eine andere Art und Weise auf die Terminal-Server-Schnittstelle zugreifen. Sie gilt auch immer dann für die Konsole, wenn die Einheit zurückgesetzt wird. Der Name und das Kennwort des Sicherheitsprofile „Default“ können nicht geändert werden; Sie sollten jedoch sämtliche Operationsprivilegien deaktivieren.

Mit den folgenden Schritten können Sie das Sicherheitsprofil „Default“ so ändern, daß nur Lesezugriffsrechte gewährt werden:

1. Öffnen Sie das Menü „Security“ im Menü „System“.
2. Öffnen Sie das Sicherheitsprofil „Default“.
3. Legen Sie für den Parameter „Operations“ den Wert „No“ fest.

   ```
   Operations=No
   ```

   Bei diesem Wert werden alle anderen Privilegien auf „N/A“ gesetzt und stehen somit nicht zur Verfügung.
4. Schließen Sie das Sicherheitsprofil „Default“.

Von jetzt an können Benutzer, die auf den Pipeline-Terminal-Server zugreifen, keinerlei Änderungen der Pipeline-Konfiguration mehr vornehmen oder Operationen ausführen, für die Zugriffsbeschränkungen gelten. Für alle Benutzer, für die die Standard-Sicherheitsstufe („Default“) gilt, werden die Kennwörter in der Pipeline-Benutzerschnittstelle durch die Zeichen „*SECURE*“ verborgen.

Ändern der SNMP-Community-Zeichenfolge für den Lese- und Schreibzugriff

Die Standardeinstellung für die SNMP-Community-Lese- und Schreib-Zeichenfolge lautet „write“.

Die SNMP-Community-Zeichenfolgen müssen von SNMP-Manager-Anwendungen angegeben werden, um auf die MIB (Management Information Base) zugreifen zu können. Die Pipeline hat zwei Community-Zeichenfolgen, die in den folgenden Parametern festgelegt werden können:

- „Read Comm“

  Der Standardwert für diesen Parameter lautet „public“. Damit ist der SNMP-Manager in der Lage, Lesebefehle (GET und GET NEXT) zu verwenden, um bestimmte Informationen anzufordern.
- „R/W Comm“

  Der Standardwert für diesen Parameter lautet „write“. Damit ist der SNMP-Manager in der Lage, sowohl Lese- als auch Schreibbefehle (GET, GET NEXT und SET) auszuführen, so daß die Anwendung auf Management-Informationen zugreifen, Alarmgrenzwerte festlegen und einige der Pipeline-Einstellungen ändern kann.

Hinweis: Da der SNMP-Schreibzugriff nicht deaktiviert werden kann, müssen Sie den Wert des Parameters „R/W Comm“ ändern, um die Pipeline vor einem unbefugten SNMP-Zugriff zu schützen.

Wenn Sie die Community-Zeichenfolge für den Lese- und Schreibzugriff ändern wollen, ist wie folgt vorzugehen:

1. Öffnen Sie das Ethernet-Profil („Ethnet-->Mod Config“).
2. Öffnen Sie das Untermenü „SNMP Options“.
3. Geben Sie einen maximal 16 Zeichen langen Wert in den Parameter „R/W Comm“ ein.

   Beispiel:

   ```
   R/W Comm=eindeutiger_wert
   ```
4. Schließen Sie das Ethernet-Profil („Ethnet-->Mod Config“).

Festlegen eines Telnet-Kennworts

Um unbefugte Telnet-Sitzungen zu vermeiden, ist die Festlegung eines Telnet-Kennworts zu empfehlen. Das Telnet-Kennwort kann bis zu 20 Zeichen lang sein und muß von jedem Benutzer angegeben werden, der eine Telnet-Verbindung zur Pipeline herstellen will.

Zur Zuweisung eines Telnet-Kennworts sind die folgenden Schritte auszuführen:

1. Öffnen Sie das Ethernet-Profil („Ethnet-->Mod Config“).
2. Geben Sie ein maximal 20 Zeichen langes Telnet-Kennwort ein.

   Beispiel:

   ```
   Telnet PW=telnet-kennwort
   ```
3. Schließen Sie das Ethernet-Profil („Ethnet-->Mod Config“).

Festlegen, daß für ankommende Verbindungen ein Profil vorhanden sein muß

Es gibt eine Vielzahl von Authentifizierungsverfahren, die Sie für ankommende Verbindungen festlegen können (siehe dazu „Verbindungssicherheit“ auf Seite 9-13). Als einfachste Stufe kann jedoch festgelegt werden, daß die Pipeline alle ankommenden Verbindungen zurückweist, für die es kein passendes Verbindungsprofil gibt.

Mit den folgenden Schritten legen Sie fest, daß ankommende Rufe nur angenommen werden, wenn ein entsprechendes Profil konfiguriert wurde:

1. Öffnen Sie das „Answer“-Profil.
2. Legen Sie für den Parameter „Profile Reqd“ den Wert „Yes“ fest.

   ```
   Profile Reqd=Yes
   ```
3. Schließen Sie das „Answer“-Profil.

Deaktivieren der Verwendung von ICMP-Redirect-Paketen

Mit ICMP kann auf dynamische Art und Weise die effizienteste IP-Route zu einem bestimmten Ziel gefunden werden. Die Verwendung von ICMP-Redirect-Paketen ist eine der ältesten Routenfindungsmethoden im Internet. Da es jedoch möglich ist, ICMP-Redirects zu fälschen und die Art und Weise, wie ein Gerät Pakete weiterleitet, zu ändern, ist dies auch eine der unsichersten Methoden. Soll die Pipeline als IP-Router agieren, empfehlen wir, die Verwendung von ICMP-Redirect-Paketen zu deaktivieren.

Mit den folgenden Schritten können Sie die Pipeline so konfigurieren, daß sie ICMP-Redirect-Pakete ignoriert:

1. Öffnen Sie das Ethernet-Profil („Ethnet-->Mod Config“).
2. Legen Sie fest, daß die Pipeline ICMP-Redirect-Pakete ignoriert.

   ```
   ICMP Redirects=Ignore
   ```
3. Schließen Sie das Ethernet-Profil („Ethnet-->Mod Config“).

Pipeline-Sicherheitsprofile

Bei der Auslieferung der Pipeline ab Werk sind die Sicherheitsprivilegien so eingestellt, daß Sie die Pipeline ohne jede Einschränkung konfigurieren und einrichten können. Im Abschnitt „Empfohlene Sicherheitsmaßnahmen“ auf Seite 9-2 werden einige Änderungen der beiden vordefinierten Sicherheitsprofile empfohlen.

Standard-Sicherheitsstufe (Sicherheitsprofil „Default“)

Die Pipeline verfügt, einschließlich der Standard-Sicherheitsstufe, über drei mögliche Sicherheitsstufen. Das Sicherheitsprofil „Default“ hat kein Kennwort. Diese Sicherheitsstufe ist stets für alle Benutzer aktiviert, die eine Telnet-Verbindung zur Einheit aufbauen oder auf eine andere Art und Weise auf die Terminal-Server-Schnittstelle zugreifen. Sie wird auch für die Konsole aktiviert, wenn die Einheit zurückgesetzt wird. Das heißt, daß die im Sicherheitsprofil „Default“ festgelegten Privilegien allgemein zugänglich sind.

Wir empfehlen Ihnen, im Sicherheitsprofil „Default“ „Operations=No“ festzulegen (siehe dazu „Empfohlene Sicherheitsmaßnahmen“ auf Seite 9-2).

Sicherheitsprofil-Kennwörter

Bei der Verwendung von Kennwörtern in Ascend-Einheiten spielt die Groß- oder Kleinschreibung keine Rolle. Das Kennwort „mein_Kennwort“ kann genauso gut auch als „mein_kennwort“ oder „MEIN_KENNWORT“ eingegeben werden.

Benutzer, die nicht über das „Edit Security“-Privileg verfügen (siehe nächster Abschnitt), können zwar in die Pipeline-Menüs Einsicht nehmen, die Kennwörter bleiben Ihnen jedoch durch die Zeichenfolge „*SECURE*“ verborgen. Wenn der Benutzer über das „Edit Security“-Privileg verfügt, sind die Kennwörter in den Sicherheitsprofilen für ihn sicht- und lesbar.

Sicherheitsprivilegien

Die anderen acht Sicherheitsprofile können jede beliebige Kombination der folgenden Privilegien enthalten:

- „Operations“
  Wenn „Operations=Yes“ festgelegt wurde, können die Parametereinstellungen durch die Benutzer geändert werden. Auch der Zugriff auf die meisten DO-Befehle ist möglich.
- „Edit Security“
  Benutzer, für die „Edit Security=Yes“ festgelegt wurde, können die Sicherheitsprofile ändern. Sie können sich sämtliche Kennwörter in den Sicherheitsprofilen anzeigen lassen. Dies ist das mit den größten Befugnissen ausgestattete Privileg, das Sie zuweisen können, da es den Benutzer in die Lage versetzt, seine eigenen Privilegien nach Belieben zu ändern. Wird „Edit Security=No“ festgelegt, sind alle Kennwörter durch die Zeichenfolge „*SECURE*“ verborgen.
- „Edit System“
  Benutzer mit dem Privileg „Edit System=Yes“ können das Systemprofil und andere systemweite Einstellungen bearbeiten.
- „Field Service“
  Wenn im Sicherheitsprofil „Field Service=Yes“ festgelegt wurde, können Benutzer von Ascend zur Verfügung gestellte Operationen für den Außendienst, wie z. B. das Laden neuer Systemsoftware in die Pipeline, ausführen. „Field Service“-Operationen sind spezielle Diagnoseroutinen, auf die nicht über die Pipeline-Menüs zugegriffen werden kann.

Ausführliche Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Das Sicherheitsprofil „Full Access“

Das Sicherheitsprofil „Full Access“ sollte für den Superuser reserviert sein, also für Sie selbst und jeden, der für das Ändern der Pipeline-Konfiguration, das Testen der Leitungen, das Wählen entfernter Standorte, das Zurücksetzen der Einheit, das Aktualisieren von Systemsoftware usw. zuständig ist.

Hinweis: Wir empfehlen Ihnen, das geänderte „Full Access“-Kennwort aufzuschreiben und an einem sehr sicheren Ort aufzubewahren. Wenn Sie alle anderen Sicherheitsstufen beschränken und dann das „Full Access“-Kennwort vergessen, sollten Sie sich mit dem Technischen Kundendienst von Ascend in Verbindung setzen.

Für das Sicherheitsprofil „Full Access“ gelten die folgenden Standardeinstellungen:

```
Name=Full Access
Passwd=Ascend
```

Hinweis: Wir empfehlen, dieses Standard-Kennwort zu ändern. Siehe dazu „Empfohlene Sicherheitsmaßnahmen“ auf Seite 9-2.

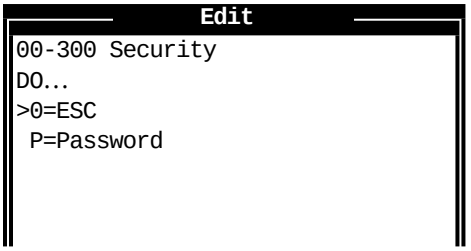
```
Operations=Yes
Edit Security=Yes
```

Hinweis: Denken Sie daran, daß das „Edit Security“-Privileg nicht deaktiviert werden darf, da die Privilegien andernfalls nicht mehr geändert werden können, wenn „Full Access“ aktiviert ist!

```
Edit System=Yes
Field Service=Yes
```

Wenn Sie sich bei der Pipeline anmelden, können Sie die Einstellungen nur lesen, nicht aber ändern, da das Standard-Sicherheitsprofil („Default“) aktiv ist. Um Änderungen vorzunehmen oder administrative Aufgaben auszuführen, müssen Sie das Profil „Full Access“ im DO-Menü aktivieren.

1 Drücken Sie die Tastenkombination Strg-D, um das DO-Menü zu öffnen, und drücken Sie dann die Taste P (oder wählen Sie „P=Password“).



2 Wählen Sie aus der sich daraufhin öffnenden Liste der Sicherheitsprofile den Eintrag „Full Access“.

Sie werden zur Eingabe des Kennworts aufgefordert.

3 Geben Sie das Kennwort für das Profil „Full Access“ ein, und drücken Sie die Eingabetaste.

Definieren neuer Sicherheitsprofile

Wenn keine anderen Benutzer die Konfigurationsprofile der Pipeline ändern oder administrative Aufgaben in der Pipeline ausführen können sollen, brauchen außer den beiden Sicherheitsprofilen „Default“ und „Full Access“ keine weiteren Sicherheitsprofile definiert zu werden. Oftmals werden aber doch zusätzliche Sicherheitsstufen definiert, um bestimmten Benutzern die Möglichkeit zu geben, zusätzliche Aufgaben auszuführen.

Wenn Sie weitere Sicherheitsprofile definieren wollen, gehen Sie wie folgt vor:

1 Öffnen Sie das Menü „Security“ im Menü „System“.

2 Öffnen Sie ein unbenanntes Profil.

3 Geben Sie einen maximal 16 Zeichen langen Namen für das Profil an.

Beispiel:

```
Name=Calabasas
```

4 Geben Sie ein neues Kennwort ein, und drücken Sie dann die Eingabetaste.

Die Pipeline verbirgt das von Ihnen eingegebene Kennwort durch Anzeigen der Zeichenfolge „*SECURE*“.

```
Passwd=*SECURE*
```

5 Legen Sie die gewünschten Privilegien fest.

Beispiel:

```
Name=Calabasas
Passwd=*SECURE*
Operations=Yes
Edit Security=No
Edit System=No
Field Service=No
```

6 Schließen Sie das neue Sicherheitsprofil.

Verbindungssicherheit

Für die Verbindungssicherheit gibt es zwei Sicherheitsstufen: Authentifizierungsmechanismen für die Kontrolle des befugten Zugangs und Netzwerksicherheitsmaßnahmen für den Schutz vor unbefugtem Zugriff auf das WAN.

Alle Authentifizierungsverfahren beruhen darauf, daß die Pipeline ein passendes Profil finden muß, um die von der rufenden Seite gesendeten Informationen zu überprüfen.

- Authentifizierungsmechanismen

  Bei der Kennwort-Authentifizierung muß die rufende Seite einen Namen und ein Kennwort angeben.

  Bei der CLID-Authentifizierung (Calling-Line ID) muß der Ruf die entsprechenden CLID-Informationen enthalten. Dadurch wird sichergestellt, daß nur Rufe von bekannten Telefonnummern angenommen werden.

  Beim Leistungsmerkmal Rückruf („Callback“) wird die Pipeline angewiesen, aufzuhängen und die rufende Seite zurückzurufen, bevor eine Kennwort-Authentifizierung stattfindet. Dieses Verfahren bietet das größte Maß an Einflußnahme darauf, daß ankommende Rufe nur angenommen werden, wenn sie von bekannten Netzwerkbenutzern ausgehen.

Hinweis: Für jede dieser Authentifizierungsverfahren wird ein konfiguriertes Profil benötigt. Im Abschnitt „Empfohlene Sicherheitsmaßnahmen“ auf Seite 9-2 finden Sie Informationen dazu, wie Sie die Pipeline unabhängig vom verwendeten Authentifizierungsverfahren so konfigurieren können, daß für jeden Ruf ein entsprechendes Profil vorhanden sein muß.

- Netzwerksicherheit

  Die Verwendung von Filtern ist eine der effektivsten Methoden, um Ihr System vor unerwünschtem WAN-Zugriff zu schützen. Dieses Kapitel geht nur kurz auf das Thema Filter ein. Ausführliche Informationen finden Sie im Kapitel 10, „Definieren von Filtern“.

PAP- und CHAP-Authentifizierung

Für PAP (Password Authentification Protocol) und CHAP (Challenge Handshake Authentification Protocol) muß das PPP-Einkapselungsverfahren eingestellt sein. Diese Authentifizierungsprotokolle gelten für PPP-, MP- und MP+-Verbindungen zur Pipeline. Beide Seiten der Verbindung müssen dasselbe Protokoll unterstützen.

PAP stellt eine einfache Methode dar, beim ersten Erstellen einer Verbindung während des bidirektionalen Handshakes die Identität mitzuteilen. Sie sendet Kennwörter im Klartext, ist also als Authentifizierungsverfahren nicht sehr leistungsfähig. PAP bietet ein gewisses Maß an Grundsicherheit, wenn Ihr System mit nicht von Ascend stammenden Geräten kommuniziert.

CHAP ist als Authentifizierungsverfahren leistungsfähiger als PAP. Bei diesem Verfahren wird während des Aufbaus der Verbindung die Identität eines Peers mittels eines Drei-Wege-Handshakes überprüft. CHAP sendet Kennwörter, die mittels einer Einwege-Hash-Funktion verschlüsselt wurden. Durch die Verwendung einer sich inkrementell verändernden Kennung und eines Variablenabfragewertes ist der Schutz gegen Playback-Angriffe von außen gesichert.

Hinweis: Neben der Festlegung, ob die PAP- oder die CHAP-Authentifizierung verwendet werden soll, gibt es weitere Parameter (z. B. in den Menüs „Telco options“ und „Session options“), die Einfluß darauf haben, ob die Pipeline in der Lage ist, die Verbindung aufzubauen. Wenn z. B. mit dem Parameter „AnsOrig“ festgelegt wurde, daß keine ankommenden Rufe angenommen werden, wird der Zustand, in dem die Pipeline einen ankommenden Ruf mit diesem Profil authentifiziert, gar nicht erst erreicht.

In Tabelle 9-1 sind die PAP- und CHAP-Parameter aufgeführt.

Tabelle 9-1: Parameter für die PAP- und CHAP-Authentifizierung

Ort	**Parameter mit Beispielwerten**
System > Sys Config (Systemprofil)	Name=meingw
Ethernet > Answer > Encaps... (Antwortprofil)	PPP=Yes MPP=Yes
Ethernet > Answer > PPP options...	Recv Auth=Either
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Station=einwahlgw Encaps=PPP (oder MPP)
Ethernet > Connections > *alle Profile* > Encaps options...	Recv PW=*SECURE* Send Auth=CHAP Send PW=*SECURE*
Ethernet > Names/Passwords > *alle Profile* (Password Profile)	Name=Fred Recv PW=*SECURE*

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Überprüfung des Namens und des Kennworts

Während der Authentifizierung benötigt das rufende Gerät oft auch den Namen und das Kennwort der Pipeline. Der Name der Pipeline wird im Systemprofil festgelegt. Der Wert des Parameters „Send PW“ ist ein Kennwort, das an das rufende Gerät gesendet wird.

Wenn der Parameter „Recv Auth“ im Antwortprofil den Wert „Either“ hat, verwendet die Pipeline zur Authentifizierung entweder PAP oder CHAP, je nachdem, welches dieser Verfahren von der rufenden Seite unterstützt wird. Wird als Wert nur „PAP“ festgelegt, weist die Pipeline alle CHAP-Kennwörter ab (und umgekehrt).

Empfängt die Pipeline einen PPP-Ruf, sucht sie in den konfigurierten Verbindungsprofilen nach einer Übereinstimmung mit dem von der rufenden Seite gesendeten Namen und dem Kennwort. Kann sie kein passendes Profil finden, wird der Ruf beendet. Hat die Pipeline jedoch ein passendes Profil gefunden, führt sie eine PAP- bzw. CHAP-Authentifizierung durch und baut dann die Verbindung auf.

Hinweis: Was zu tun ist, wenn die rufende Seite eine IP-Adresse sendet oder die dynamische Zuweisung einer IP-Adresse anfordert, können Sie dem folgenden Abschnitt („Zusätzliche Schritte bei IP-Routing-Verbindungen“) entnehmen.

Zusätzliche Schritte bei IP-Routing-Verbindungen

Zur Authentifizierung einer IP-Routing-Verbindung wird vor dem Aufbau eines Rufes bei der PPP-Aushandlung die IP-Adresse überprüft.

Wenn die PPP-Software der rufenden Seite eine IP-Adresse sendet, muß die Pipeline ein Verbindungsprofil finden, das dieser Adresse entspricht. Gelingt ihr das nicht, wird der Ruf ohne PAP- bzw. CHAP-Authentifizierung beendet. Wird dagegen ein passendes Profil gefunden, erfolgt eine PAP- bzw. CHAP-Authentifizierung, und die Verbindung wird aufgebaut.

In Tabelle 9-2 finden Sie eine Aufstellung der IP-Parameter, die sich auf die PPP-Aushandlung auswirken können.

Tabelle 9-2: Zusätzliche IP-Parameter mit Auswirkungen auf die PPP-Aushandlung

Ort	Parameter mit Beispielwerten
Ethernet > Answer > PPP options...	Route IP=Yes
Ethernet > Connections > *alle Profile* > IP options...	LAN Adrs=10.5.6.7/24

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Informationen zu IP-Routing-Verbindungen entnehmen Sie bitte Kapitel 7, „Konfigurieren der Pipeline als IP-Router“.

CLID-Authentifizierung

CLID ist die Abkürzung für „Calling Line ID“ (Anschlußkennung der rufenden Leitung) und gibt damit die Telefonnummer des rufenden Geräts an. Die CLID-Authentifizierung sorgt dafür, daß nur ankommende Rufe angenommen werden, die von einer bekannten Telefonnummer ausgehen. In der Tabelle 9-3 werden alle Parameter aufgeführt, die sich auf die CLID-Authentifizierung auswirken.

Tabelle 9-3: Parameter für die CLID-Authentifizierung

Ort	Parameter mit Beispielwerten
Ethernet > Answer (Antwortprofil)	ID Auth=Required
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Calling #=555-1213

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Beim CLID-Authentifizierungsverfahren beendet die Pipeline den Ruf, wenn die im Parameter „Calling #“ angegebene Nummer nicht mit der Nummer der rufenden Seite übereinstimmt. Die CLID-Authentifizierung wird vor der Überprüfung von Namen bzw. Kennwörtern durchgeführt. Kann die Pipeline die Nummer der rufenden Seite in keinem ihrer Profile finden, hängt sie auf.

Hinweis: In bestimmten Installationen kann es möglich sein, daß der WAN-Provider CLIDs nicht zur Verfügung stellen kann, oder das einzelne Teilnehmer ihre CLIDs geheimhalten möchten. Für die CLID-Authentifzierung muß der Ruf außerdem von Ende zu Ende über ISDN laufen, und der WAN-Provider muß die automatische Rufnummernidentifizierung (Automatic Number Identification, ANI) zur Verfügung stellen. Fragen Sie Ihren WAN-Provider, ob die Rufnummer des A-Teilnehmers über das Netz an den B-Teilnehmer weitergeleitet wird. In einigen Fällen gibt das Netz die Rufnummer der rufenden Seite nicht weiter, z. B. dann, wenn die Pipeline an eine oder mehrere Nebenstellenanlagen angeschlossen ist.

Der Parameter „ID Auth“ im Antwortprofil kann die folgenden Werte haben:

- „ID Auth=Ignore“

  „Ignore“ gibt an, daß die Rufnummer der rufenden Seite für die Authentifizierung nicht benötigt wird.

- „ID Auth=Prefer“

  „Prefer“ gibt an, daß für einen Aufbau des Rufes die Rufnummer der rufenden Seite mit dem Wert des Parameters „Calling #“ übereinstimmen muß, falls die CLID verfügbar ist. Ist die CLID nicht verfügbar oder kann die Pipeline kein passendes Profil finden, verwendet sie zur Authentifizierung den Parameter „Recv Auth“ bzw. „Password Reqd“.

- „ID Auth=Required“

  „Required“ gibt an, daß die Rufnummer der rufenden Seite mit dem Wert des Parameters „Calling #“ übereinstimmen muß, damit die Pipeline den Ruf beantwortet. Ist die CLID nicht verfügbar, wird der Ruf nicht beantwortet.

Rückruf-Sicherheit

Wenn das Leistungsmerkmal „Rückruf“ (Parameter „Callback“) aktiviert ist, hängt die Pipeline ankommende Rufe sofort auf und wählt selbst eine Verbindung zum rufenden Gerät. In der Tabelle 9-4 werden die Rückruf-Parameter aufgeführt.

Tabelle 9-4: Parameter für die Rückruf-Sicherheit

Ort	Parameter mit Beispielwerten
Ethernet > Connections > *alle Profile* (Verbindungsprofil)	Calling #=555-1213 Dial #=555-1213
Ethernet > Connections > *alle Profile* > Telco options...	Callback=Yes AnsOrig=Both

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

Das Leistungsmerkmal Rückruf gewährleistet, daß nur Verbindungen mit der im Parameter „Calling #“ angegebenen Rufnummer zustandekommen.

Wird „Callback=Yes“ festgelegt, muß für den Parameter „AnsOrig“ der Wert „Both“ angegeben werden, da die Pipeline den Ruf sowohl beantworten als auch eine Verbindung zu dem Gerät aufbauen muß, das auf sie zugreifen möchte. Auch das rufende Gerät muß Rufe sowohl initiieren als auch von der Pipeline initiierte ankommende Rufe beantworten können.

Hinweis: Der Parameter „Callback“ ist für Mietleitungen (Call Type=Nailed) nicht verfügbar (Callback=N/A).

Mit den folgenden Schritten können Sie die Rückruf-Sicherheit einrichten:

1. Öffnen Sie ein Verbindungsprofil.
2. Geben Sie die Nummer an, die die Pipeline wählen soll, um die andere Seite der Verbindung zu erreichen.

   Beispiel:

   ```
   Dial #=555-1213
   ```

3 Geben Sie die Nummer an, von der aus das rufende Gerät einen Ruf initiiert, um die Pipeline zu einem Rückruf aufzufordern.

Beispiel:

```
Calling #=555-1213
```

4 Öffnen Sie das Untermenü „Telco Options“.

5 Aktivieren Sie die Rückruf-Sicherheit.

```
Callback=Yes
AnsOrig=Both
```

6 Schließen Sie das Verbindungsprofil.

Netzwerksicherheit

Die Netzwerksicherheit gilt für über eine WAN-Verbindung ankommende Pakete. In diesem Abschnitt werden die folgenden beiden Netzwerksicherheitsmechanismen beschrieben:

- Filter
- Beschränkung des SNMP-Zugriffs

Empfehlungen zur Verwendung von ICMP-Redirect-Paketen finden Sie im Abschnitt „Empfohlene Sicherheitsmaßnahmen“ auf Seite 9-2.

Filter

Im Kapitel 10, „Definieren von Filtern“, wird beschrieben, wie Filterprofile organisiert sind und wie sie erstellt werden. Dieser Abschnitt gibt einen Überblick darüber, wie Filterprofile zum Zwecke der Netzwerksicherheit eingesetzt werden können.

Bei den Filtern zur Gewährleistung der Netzwerksicherheit handelt es sich um Datenfilter, die auf ankommende oder/und abgehende Datenströme angewendet werden können. Mit Datenfiltern kann verhindert werden, daß bestimmte Pakete das lokale Netzwerk erreichen oder aber das lokale Netzwerk verlassen und über das WAN versendet werden. So können zum Beispiel mit Hilfe von Datenfiltern Pakete abgewiesen werden, die an bestimmte Hosts adressiert sind oder die an das lokale Netzwerk gesendet wurden. Mit Filtern kann auch verhindert werden,

daß bestimmte Benutzer von außerhalb auf die Informationen in Ihrem lokalen Netzwerk zugreifen können, selbst wenn sie wissen, wie ein Filter umgangen werden kann. So können Sie zum Beispiel einen Filter definieren, der ankommende Pakete aussondert, deren Ausgangsadresse sich im lokalen Netzwerk befindet bzw. eine Rückschleifadresse ist.

Jeder Filter besteht aus einer geordneten Liste von Kriterien auf der Grundlage von entweder IP-spezifischen oder protokollunabhängigen Informationen. Mit IP-Filtern können Pakete aufgrund der folgenden Kriterien (auch in beliebiger Kombination) gefiltert werden:

- Ausgangsadresse
- Zieladresse
- Protokollnummer
- Ausgangsanschluß
- Zielanschluß
- ob eine TCP-Sitzung aufgebaut wurde

Bei protokollunabhängigen Filtern können Datenwerte und Masken angegeben werden, die die Pipeline verwendet, um festzulegen, ob ein Paket ausgesondert oder weitergeleitet werden soll.

Sicherheitskarten (Token Security)

Sichere Netzwerke können so eingerichtet werden, daß ihr Kennwort sich sehr häufig, z. B. mehrere Male pro Tag, ändert. Das Kennwort wird dabei durch einen externen Authentifizierungsserver, wie z. B. von Security Dynamics (ACE) oder Enigma Logic (SAFEWORD), geändert und mit der persönlichen Sicherheitskarte des Benutzers (Gerät in der Form und Größe einer Kreditkarte) synchronisiert, damit dieser jederzeit und sofort das jeweils aktuelle Kennwort zur Verfügung hat. Das aktuelle, nur für den jeweiligen Moment gültige Kennwort wird auf der LCD-Anzeige der Sicherheitskarte angezeigt, so daß der Benutzer auf das sichere Netzwerk zugreifen kann.

Für diese sicheren Netzwerke agiert die Pipeline als Client eines zentralen Servers, wie z. B. eines MAX 4000, der als ein NAS (Network Access Server)

fungiert. Der NAS ist ein Client eines RADIUS-Servers, der wiederum als Client des ACE- bzw. SAFEWORD-Servers auftritt.

Abbildung 9-1 zeigt ein Beispiel für eine Sicherheitskartenumgebung. Der Benutzer, der einen Ruf über die Pipeline initiiert, ist ein Client der Pipeline, die wiederum ein Client der MAX-Einheit (als NAS agierend) ist. Der NAS fordert die Authentifizierung vom RADIUS-Server an, der dann mit dem externen Server in Kontakt tritt.

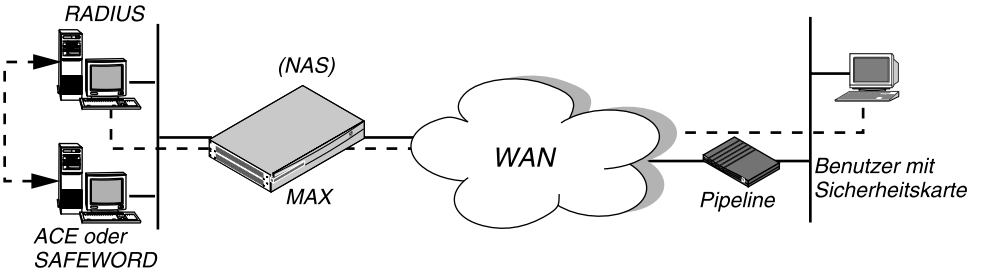


Abbildung 9-1: RADIUS-Server als Client des ACE- bzw. SAFEWORD-Servers

Wenn ein Benutzer auf ein sicheres Netzwerk zugreifen will, treten die folgenden Ereignisse auf:

1 Die rufende Einheit (z. B. eine Ascend Pipeline) stellt eine Verbindung zum NAS (die MAX-Einheit) her.

2 Der NAS fordert beim RADIUS-Server die Authentifizierung des Rufes an.

3 Der RADIUS-Server leitet die Anforderung an einen ACE- bzw. SAFEWORD-Server weiter.

4 Der ACE- bzw. SAFEWORD-Server sendet eine Kennwort-Abfrage (auch ein Null-Kennwort ist möglich) über den RADIUS-Server und den NAS zur rufenden Einheit zurück.

5 Der Benutzer im entfernten Netzwerk antwortet auf die Kennwort-Abfrage, indem er das aktuelle Kennwort sendet, das er der Anzeige auf seiner Sicherheitskarte entnehmen kann.

Hinweis: Nähere Informationen zum Senden von Sicherheitskarten-Kennwörtern durch den Benutzer finden Sie im Abschnitt „Authentifizierung von abgehenden Rufen mit Hilfe von Sicherheitskarten“ auf Seite 9-23.

Wenn der Benutzer das richtige Kennwort sendet, kann er auf das Netzwerk zugreifen.

Nach Ablauf von 60 Sekunden ohne Beantwortung der Kennwortabfrage wird der Ruf beendet.

Wird ein falsches Kennwort eingegeben, fordert der ACE- bzw. SAFEWORD-Server erneut zur Angabe des Kennworts auf. Wenn zum dritten Mal ein falsches Kennwort eingegeben wurde oder dreimal 60 Sekunden lang keine Eingabe erfolgte, wird der Ruf beendet.

Authentifizierung von abgehenden Rufen mit Hilfe von Sicherheitskarten

Sie können die Pipeline als rufende Einheit konfigurieren, um Inhabern einer Sicherheitskarte im lokalen Netzwerk zu gestatten, sich über einen NAS in ein sicheres Netzwerk einzuwählen. In diesem Abschnitt wird beschrieben, welche Schritte auszuführen sind, um die Pipeline so zu konfigurieren, daß sie Rufe zu einem entfernten NAS aufbauen und Kennwortabfragen vom NAS beantworten kann.

Einrichten einer abgehenden Verbindung zu einem sicheren Netzwerk

Damit die Pipeline Rufe zu einem NAS in einem sicheren Netzwerk initiieren kann, muß ein entsprechendes Verbindungsprofil vorhanden sein, in dem ein Authentifizierungsmodus auf Tokenbasis festgelegt wurde.

Davon, welcher Authentifizierungsmodus in der rufenden Einheit konfiguriert wurde, hängt ab, wie die Token-Kennwörter übertragen werden und welche Auswirkungen das Hinzufügen von Kanälen zu hergestellten Sitzungen auf den sich einwählenden Benutzer hat.

Die rufende Einheit fordert den Authentifizierungsmodus an, mit dem sie konfiguriert ist, aber vom RADIUS-Dämonen und dem Benutzerprofil, auf das der antwortende NAS zugreift, hängt es ab, welcher Modus tatsächlich verwendet wird.

PAP-TOKEN-Modus

PAP-TOKEN, eine Erweiterung der PAP-Authentifizierung, ist der Standard-Authentifizierungsmodus, wenn das RADIUS-Profil ein ACE- oder SAFEWORD-Kennwort hat.

Bei Verwendung des PAP-TOKEN-Modus wird das vom Benutzer eingegebene dynamische Kennwort im Klartext (über PAP) gesendet. Da es sich aber um ein nur einmal zu benutzendes Kennwort handelt, stellt dies kein ernstes Sicherheitsrisiko dar.

Die Antwort auf die erste Kennwortabfrage authentifiziert den Basiskanal des Rufes. Wenn die Bandbreite durch einen weiteren Kanal erweitert werden soll, muß für jeden hinzuzufügenden Kanal ein Kennwort eingegeben werden.

Für PAP-TOKEN müssen in der rufenden Einheit die folgenden Parameter konfiguriert werden:

Tabelle 9-5: PAP-TOKEN-Parameter

Ort	**Parameter mit Beispielwerten**
Ethernet > Connections > *alle Profile* > Encaps options... (Verbindungsprofil)	Send Auth=PAP-TOKEN `Send PW=*SECURE*`

Der Parameter „Send Auth“ gibt an, welcher Authentifizierungsmodus von der rufenden Seite angefordert wird („PAP-TOKEN“). Das im Parameter „Send PW“ angegebene Kennwort wird während der Aushandlung der Sitzungsbedingungen gesendet. Wenn die Sitzung dann nach dem Kennwort fragt, gibt der Benutzer sein aktuelles, nur einmal gültiges Kennwort gemäß der Anzeige der Sicherheitskarte ein.

PAP-TOKEN-CHAP-Modus

Wenn in der rufenden Einheit „PAP-TOKEN-CHAP“ festgelegt, das RADIUS-Profil am anderen Ende der Verbindung jedoch nicht für PAP-TOKEN-CHAP eingerichtet wurde, wird statt dessen PAP-TOKEN verwendet. Bei PAP-TOKEN-CHAP werden zusätzlich hinzugefügte Kanäle mit Hilfe von CHAP authentifiziert.

Das vom Benutzer eingegebene dynamische Kennwort wird zur Authentifzierung des Basiskanals des Rufes verwendet. Es wird im Klartext (über PAP) gesendet. Wenn die Pipeline dem Basiskanal des Rufes weitere Kanäle hinzufügt, werden diese bei Verwendung von PAP-TOKEN-CHAP jeweils mit Hilfe der CHAP-Authentifizierung authentifiziert. CHAP sendet verschlüsselte Kennwörter, so daß es das Hilfskennwort aus dem Parameter „Aux Send PW“ nehmen und sicher übertragen kann.

Mit den folgenden Parametern können Sie die rufende Einheit für den PAP-TOKEN-CHAP-Modus konfigurieren:

Tabelle 9-6: PAP-TOKEN-CHAP-Parameter

Ort	**Parameter mit Beispielwerten**
Ethernet > Connections > *alle Profile* > Encaps options... (Verbindungsprofil)	Send Auth=PAP-TOKEN-CHAP `Send PW=*SECURE*` Aux Send PW=*SECURE*

Der Parameter „Send Auth“ gibt an, welcher Authentifizierungsmodus von der rufenden Seite angefordert wird („PAP-TOKEN-CHAP“). Das im Parameter „Send PW“ angegebene Kennwort wird während der Aushandlung der Sitzungsbedingungen gesendet. Wenn die Sitzung dann nach dem Kennwort fragt, gibt der Benutzer sein aktuelles, nur einmal gültiges Kennwort gemäß der Anzeige der Sicherheitskarte ein.

Der Parameter „Aux Send PW“ dient zur CHAP-Authentifizierung von zusätzlich zugewiesenen Kanälen.

CACHE-TOKEN-Modus

„CACHE-TOKEN“ verwendet das Protokoll CHAP und speichert das anfänglich eingegebene Kennwort für die Wiederverwendung zur Authentifizierung von hinzuzufügenden Kanälen in einem Zwischenspeicher. Im RADIUS-Profil am anderen Ende der Verbindung muß festgelegt werden, wie lange das Token zwischengespeichert werden soll.

Für den CACHE-TOKEN-Modus müssen die folgenden Parameter in der rufenden Einheit konfiguriert sein:

Tabelle 9-7: CACHE-TOKEN-Parameter

Ort	Parameter mit Beispielwerten
Ethernet > Connections > *alle Profile* > Encaps options... (Verbindungsprofil)	Send Auth=CACHE-TOKEN `Send PW=*SECURE*`

Der Parameter „Send Auth“ gibt an, welcher Authentifizierungsmodus von der rufenden Seite angefordert wird (CACHE-TOKEN). Das im Parameter „Send PW“ angegebene Kennwort wird während der Aushandlung der Sitzungsbedingungen gesendet. Dann wird der Benutzer aufgefordert, ein Token-Kennwort zur CHAP-Authentifizierung des Basiskanals einzugeben. Wurde der RADIUS-Server richtig konfiguriert, speichert er dieses verschlüsselte Kennwort für den angegebenen Zeitraum bzw. für die angegebene Zeit der Inaktivität während der Verbindung zwischen. Wenn dem Ruf Kanäle hinzugefügt werden oder ein neuer Ruf aufgebaut wird, wird für die Authentifizierung das zwischengespeicherte Kennwort verwendet.

Konfigurieren der Pipeline für APP Server

Damit die Benutzer von ihren PCs bzw. von UNIX-Hosts im lokalen Netzwerk aus Token-Kennwörter senden können, muß die Pipeline so konfiguriert werden, daß sie mit dem Dienstprogramm APP Server auf diesem Host kommunizieren kann. APP ist ein UDP-Protokoll mit dem Standardport 7001. Die Kommunikation zwischen der Pipeline und dem Host, auf dem APP Server läuft, kann entweder im Unicast-Modus (wenn sowohl die Pipeline als auch der Host eine IP-Adresse haben) oder im Broadcast-Modus (wenn der Host eventuell keine IP-Adresse hat) erfolgen.

Die APP-Parameter werden in Tabelle 9-8 aufgeführt.

Tabelle 9-8: APP-Server-Parameter

Ort	Parameter mit Beispielwerten
Ethernet > Mod Config > Auth... (Ethernet-Profil)	APP Server=Yes APP Host=10.65.212.1 APP Port=7001

Wenn die Pipeline für die Kommunikation mit APP Server eingerichtet werden soll, sind die folgenden Schritte auszuführen:

1 Öffnen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

2 Öffnen Sie das Untermenü „Auth“.

3 Aktivieren Sie den Parameter „APP Server“.

```
APP Server=Yes
```

Mit dieser Einstellung ist die Pipeline in der Lage, Kennwortabfragen an den Host zu senden, auf dem APP Server läuft.

4 Geben Sie die IP-Adresse des Hosts an, auf dem APP Server läuft.

Beispiel:

```
APP Host=10.65.212.1
```

Wenn der Host seine Adresse beim Hochfahren von einem BOOTP- oder DHCP-Server zugewiesen bekommt oder aber keine IP-Adresse hat, können Sie mit Hilfe dieses Parameters die IP-Broadcast-Adresse festlegen (255.255.255.255).

5 Geben Sie die UDP-Portnummer für die Kommunikation mit dem Host an, auf dem APP Server läuft.

Beispiel:

```
APP Port=7001
```

„7001“ ist der Standard-UDP-Port für den APP Server.

Hinweis: Wenn Sie diese Nummer ändern, müssen Sie die neue UDP-Portnummer auch im Dienstprogramm APP Server (DOS), in der Datei „win.ini“ (Windows) bzw. in der Datei „/etc/services“ (UNIX) angeben. Die Pipeline und der Host, auf dem APP Server läuft, müssen beide dieselbe UDP-Portnummer eingestellt haben.

6 Schließen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

Aufrufen des Kennwortmodus in der Pipeline

Sie können Verbindungen zu einem sicheren Netzwerk auf die übliche Art und Weise herstellen, indem Sie ein Programm aufrufen, für das eine Verbindung zu einem Host in diesem entfernten Netzwerk bestehen muß, oder indem Sie das DO-Menü in der Pipeline verwenden.

Zum Aufrufen des Kennwortmodus („Password Mode“) in einer Terminal-Server-Sitzung ist wie folgt vorzugehen:

1 Der Benutzer gibt an der Eingabeaufforderung des Terminal-Servers den folgenden Befehl ein:

```
set password
```

Es erscheint die folgende Meldung:

```
Entering Password Mode...
```

Die Eingabeaufforderung sieht daraufhin wie folgt aus:

```
[^C to exit] Password Mode>
```

2 Der Benutzer stellt die Verbindung her.

3 Beim Aushandeln der Verbindung gibt der entfernte NAS ein Aufforderung zur Kennworteingabe zurück. Diese sieht wie folgt aus:

```
From: Hostname
0-Challenge: challenge

Enter next password:
```

4 Der Benutzer gibt das Kennwort gemäß der Anzeige seiner Sicherheitskarte ein.

Zur Eingabe des richtigen Kennworts hat der Benutzer 60 Sekunden Zeit. Wurde in dieser Zeit das richtige Kennwort eingegeben, wird eine Verbindung zum sicheren Netzwerk aufgebaut. Wenn innerhalb der 60 Sekunden kein richtiges Kennwort eingegeben wurde, wird der Login-Versuch abgebrochen. Wurde ein falsches Kennwort eingegeben, wird der Benutzer insgesamt dreimal zur Eingabe des richtigen Kennworts aufgefordert.

Hostname ist der Name des gerufenen NAS, z. B. der Pipeline; bei einigen Systemen ist die Angabe dieses Wertes optional. Wenn der Parameter „Send Auth“ falsch konfiguriert wurde, erscheint keine Kennwortabfrage, bzw. es wird eine Fehlermeldung ausgegeben, wie z. B.:

```
From: Hostname
Received unexpected PAP Challenge!... check PPP Auth Mode
```

5 Um zum normalen Terminal-Server-Betrieb zurückzukehren, drückt der Benutzer im Kennwortmodus die Tastenkombination Strg-C.

APP Server 2.0

Dieses Release der Ascend-Software beinhaltet die Version 2.0 des Dienstprogramms APP Server für UNIX, DOS, Windows 3.1, Windows 95 und Windows NT.

APP Server versetzt den Benutzer in die Lage, auf Token-Kennwortabfragen von einem externen Authentifizierungsserver, wie z. B. von Security Dynamics (ACE) oder Enigma Logic (SAFEWORD), zu reagieren. Diese externen Authentifizierungsserver ändern das Kennwort täglich viele Male und synchronisieren es mit der persönlichen Sicherheitskarte des Benutzers (Gerät in der Form und Größe einer Kreditkarte), damit dieser jederzeit und sofort das jeweils aktuelle Kennwort zur Verfügung hat. Das aktuelle, nur für den jeweiligen Moment gültige Kennwort wird auf der LCD-Anzeige der Sicherheitskarte angezeigt, so daß der Benutzer auf das sichere Netzwerk zugreifen kann. Weitere Informationen zur Arbeit mit Sicherheitskarten finden Sie im Abschnitt „Sicherheitskarten (Token Security)“ auf Seite 9-21.

Bei früheren Versionen von APP Server konnten immer nur einzelne Benutzer auf von einem entfernten ACE- bzw. SAFEWORD-Server ausgehende Kennwortabfragen reagieren. Version 2.0 unterstützt Mehrfach-Tokens, sowohl für Benutzernamen als auch für das aktuelle Kennwort, so daß mit dieser Version auch mehrere Benutzer den APP-Server nutzen können, um auf Kennwortabfragen zu reagieren.

Die verschiedenen Versionen von APP Server

Das Dienstprogramm APP Server gibt es für fünf verschiedene Plattformen: DOS, Windows 3.1, Windows 95, Windows NT und UNIX. Das Dienstprogramm kann über die Adresse ftp.ascend.com als Tar-Archiv heruntergeladen werden. Die Tar-Datei enthält alle fünf Versionen des Dienstprogramms.

Die Tar-Datei legt bei der Dekomprimierung für jede Version ein eigenes Verzeichnis an, insgesamt also fünf. Der Inhalt der Verzeichnisse für die Windows 95- und Windows NT-Versionen ist komprimiert.

Die UNIX-Version wird in Form von Quelldateien geliefert.

Die DOS- und Windows-Versionen enthalten die folgenden EXE-Dateien:

- APPSRVDS.EXE (für DOS)
- APPSRV31.EXE (für Windows 3.1)
- APPSRV95.EXE (für Windows 95)
- APPSRVNT.EXE (für Windows NT)

Konfigurieren der Pipeline

Damit die Benutzer von ihren PCs bzw. von UNIX-Hosts im lokalen Netzwerk aus Token-Kennwörter senden können, muß die Pipeline so konfiguriert werden, daß sie mit dem Dienstprogramm APP Server auf diesem Host kommunizieren kann. APP ist ein UDP-Protokoll mit dem Standardport 7001. Die Kommunikation zwischen der Pipeline und dem Host, auf dem APP Server läuft, kann entweder im Unicast-Modus (wenn sowohl die Pipeline als auch der Host eine IP-Adresse haben) oder im Broadcast-Modus (wenn der Host eventuell keine IP-Adresse hat) erfolgen.

Wenn die Pipeline für die Kommunikation mit APP Server eingerichtet werden soll, sind die folgenden Schritte auszuführen:

1 Öffnen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

2 Öffnen Sie das Untermenü „Auth“.

3 Aktivieren Sie den Parameter „APP Server“.

```
APP Server=Yes
```

Mit dieser Einstellung ist die Pipeline in der Lage, Kennwortabfragen an den Host zu senden, auf dem APP Server läuft.

4 Geben Sie die IP-Adresse des Hosts an, auf dem APP Server läuft.

Beispiel:

```
APP Host=10.65.212.1
```

Wenn der Host seine Adresse beim Hochfahren von einem BOOTP- oder DHCP-Server zugewiesen bekommt oder aber keine IP-Adresse hat, können Sie mit Hilfe dieses Parameters die IP-Broadcast-Adresse festlegen (255.255.255.255).

5 Geben Sie die UDP-Portnummer für die Kommunikation mit dem Host an, auf dem APP Server läuft.

Beispiel:

```
APP Port=7001
```

„7001“ ist der Standard-UDP-Port für den APP Server.

Hinweis: Wenn Sie diese Nummer ändern, müssen Sie die neue UDP-Portnummer auch im Dienstprogramm APP Server (DOS), in der Datei „win.ini“ (Windows) bzw. in der Datei „/etc/services“ (UNIX) angeben. Die Pipeline und der Host, auf dem APP Server läuft, müssen beide dieselbe UDP-Portnummer eingestellt haben.

6 Schließen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

Festlegen von Banner-Text für die Kennwort-Eingabeaufforderung

Sie können ein Banner erstellen, mit dem Benutzer begrüßt werden, wenn eine Kennwortabfrage empfangen wird. Die Datei APPSRVR.INI in dem Verzeichnis, in dem auch APP Server installiert ist, sollte Banner-Text enthalten, der bei Eingang einer Kennwortabfrage zusammen mit der Kennwort-Eingabeaufforderung angezeigt wird. Das Banner kann bis zu 200 Zeichen und bis zu fünf Textzeilen enthalten. In der ersten Zeile der Datei muß der Text „[BANNER]“ stehen.

Beispiel:

```
[BANNER]
line1=Das Sicherheitskennwort wurde geändert. Schauen Sie
line2=auf Ihrer Karte nach und geben Sie jetzt das aktuelle
line3=Kennwort ein.
line4=Sie haben für die Eingabe des Kennworts 60 s Zeit.
```

Auf dem APP Server-Bildschirm wird unmittelbar nach dem Banner-Text die Kennwort-Eingabeaufforderung angezeigt. Der Benutzer hat 60 Sekunden Zeit, das aktuelle Kennwort von seiner Sicherheitskarte abzulesen und es fehlerfrei einzugeben.

Installation und Einsatz der UNIX-Version von APP Server

Wenn ein Benutzer eine Anwendung startet, für die eine Verbindung zu einem Host in einem sicheren Netzwerk benötigt wird, initiiert die Pipeline (wie üblich) transparent einen Ruf. Nach dem ersten Aushandeln der Sitzungsbedingungen gibt der entfernte ACE- bzw. SAFEWORD-Server eine Kennwortabfrage zurück, die ungefähr so aussieht:

```
From: Hostname
0-Challenge: Challenge (bzw. Null-Challenge, je nach Setup)
Enter next password:
```

Diese Eingabeaufforderung erscheint im APP Server-Bildschirm des UNIX-Hosts. Der Benutzer hat 60 Sekunden Zeit, das aktuelle dynamische Kennwort von seiner Sicherheitskarte abzulesen und es fehlerfrei einzugeben. Wenn mehrere Benutzer gleichzeitig den APP-Server benutzen müssen, kann der Benutzer einen Namen hinzufügen. Dazu ist folgendes Format zu verwenden:

```
Kennwort.Benutzername
```

(Ein Kennwort, gefolgt von einem Punkt, der wiederum vom Benutzernamen gefolgt wird.)

Mit den folgenden Schritten können Sie APP Server auf einem UNIX-Host installieren:

1. Bearbeiten Sie den Makefile entsprechend den Erfordernissen für Ihr Betriebssystem und Ihren Compiler.
2. Kompilieren Sie die Quelldatei „appsrvr“ („make“).
3. Fügen Sie „/etc/services“ eine Zeile hinzu, in der Sie APP Server den UDP-Port 7001 zuweisen:

   ```
   appServer<tab>7001/udp
   ```

   Wenn der Port 7001 bereits für einen anderen Zweck verwendet wird, können Sie für APP Server einen anderen Port verwenden. Dazu muß der Datei „/etc/services“ die folgende Zeile hinzugefügt werden:

   ```
   appServer<tab>nnn/udp
   ```

   nnn steht für die zu verwendende Portnummer. Dabei ist zu beachten, daß diese Nummer auch in der Pipeline angegeben werden muß.
4. Wenn der UNIX-Host eine IP-Adresse hat, können Sie APP Server im Unicast-Modus betreiben, indem Sie folgenden UNIX-Befehl eingeben:

   ```
   ./appsvr
   ```

   Im Unicast-Modus sendet APP Server Pakete über den angegebenen UDP-Port, wobei als Ausgangsadresse die IP-Adresse des APP Server-Hosts angegeben wird. Wenn die Pipeline diese Pakete über den angegebenen UDP-Port empfängt, werden Pakete an diese IP-Adresse zurückgesendet.

5 Hat der UNIX-Host *keine* IP-Adresse (z. B., wenn er seine Adresse von einem BOOTP- oder DHCP-Server zugewiesen bekommt), können Sie APP Server statt dessen im Broadcast-Modus betreiben. Geben Sie dazu den folgenden Befehl ein:

```
./appsrvr –b
```

Die Option „–b“ stellt eine Socket-Option dar, um Broadcast-Sendungen zu erlauben und Beschwerden des Dienstprogramms zu verhindern, daß ungültige APP-Rahmentypen empfangen werden, wenn es seine eigenen Sendungen empfängt.

Hinweis: Bei einigen UNIX-Systemen benötigen Sie für den Betrieb von APP Server im Broadcast-Modus „root“-Privilegien. Wenn Sie APP Server im Broadcast-Modus betreiben, ist darauf zu achten, daß der Parameter „APP Host“ der Pipeline die Broadcast-Adresse enthält (APP Host=255.255.255.255).

Installation und Einsatz der DOS-Version von APP Server

Um eine Verbindung zu einem sicheren entfernten Netzwerk aufbauen zu können, muß der DOS-Benutzer den PC neu starten. Nach der ersten Aushandlung der Verbindungsbedingungen sendet der entfernte ACE- bzw. SAFEWORD-Server eine Kennwortabfrage, die ungefähr wie folgt aussieht:

```
From: Hostname
0-Challenge: Challenge (oder Null-Challenge, je nach Setup)
Enter next password:
```

Wenn der APP-Server von mehreren Benutzern zum Einloggen in ein sicheres entferntes Netzwerk über die Pipeline verwendet wird, muß jeder der Benutzer seinen Benutzernamen mit angeben. Dazu ist das folgende Format zu verwenden:

```
Kennwort.Benutzername
```

(Ein Kennwort, gefolgt von einem Punkt, der wiederum vom Benutzernamen gefolgt wird.)

Installieren der DOS-Software

Für die DOS-Version von APP Server wird ein ODI-Treiber zur Bereitstellung der Netzwerkfunktionen benötigt. Nach dem Laden des ODI-Treibers muß dieser sofort in die Datei AUTOEXEC.BAT eingetragen werden. (Dazu muß u. U. die Datei STARTNET.BAT bearbeitet werden; die Datei NET.CFG muß in dieser Version jedoch nicht mehr geändert werden.)

Zur Installation der DOS-Version von APP Server ist wie folgt vorzugehen:

1 Erstellen Sie im Stammverzeichnis ein Verzeichnis mit dem Namen \ASCEND.

2 Kopieren Sie die Datei APPSRVDS.EXE in dieses Verzeichnis.

3 Wenn die Datei APPSRVR.INI bereits vorhanden ist, ist diese ebenfalls in das Verzeichnis zu kopieren.

Siehe „Festlegen von Banner-Text für die Kennwort-Eingabeaufforderung“ auf Seite 9-32.

4 Öffnen Sie die Datei AUTOEXEC.BAT, und fügen Sie eine Befehlszeile hinzu, mit der die Datei APPSRVDS.EXE aufgerufen wird.

Für APPSRVDS.EXE unter DOS ist kein IP-Stack und keine IP-Adresse erforderlich; es muß jedoch ein ODI-Treiber vorhanden sein.

Die Befehlszeile für APPSRVDS.EXE muß sich nach der Zeile befinden, mit der der ODI-Treiber aufgerufen wird, und vor der Zeile, die den Netzwerkprotokoll-Stack (TCP/IP oder IPX oder ein anderes unterstütztes Protokoll) enthält. Beispiel:

```
C:\NOVELL\LSL.COM
C:\NOVELL\XXXODI.COM
C:\ASCEND\APPSRVDS.EXE

REM Als nächstes wird der Protokoll-Stack geladen
```

5 Schließen Sie die Datei AUTOEXEC.BAT.

6 Führen Sie einen Neustart durch.

In der AUTOEXEC.BAT-Befehlszeile können die folgenden Optionen verwendet werden:

- /t – dient zur Angabe der Zeitverzögerung zwischen den einzelnen Verbindungsversuchen (Sekunden)
- /y – dient zur Angabe der maximalen Anzahl der Verbindungsversuche
- /m – dient zur Angabe der MAC-Adresse (dezimal) des PC, auf dem APP Server läuft
- /p – dient zur Angabe der Nummer des UDP-Ports für die Kommunikation mit der Pipeline
- /b – dient zur Angabe des UDP-Ports für Broadcast-Meldungen
- /f – unterdrückt den Ruf beim Starten
- /d – beendet den Ruf
- /c – dient zur Angabe des Namens des Verbindungsprofils für die Verbindung mit dem sicheren entfernten Netzwerk
- /? – ruft den Hilfe-Bildschirm auf

Hinweis: Der PC sendet ein Broadcast-UDP-Paket, dessen Ziel- und Ausgangs-Portnummer 7001 lautet, wenn Sie diesen Standardwert nicht mit der Option /p bzw. /b geändert haben. Wird im Parameter „APP Port“ eine andere UDP-Portnummer als 7001 angegeben, müssen Sie mit Hilfe einer dieser Optionen die Portnummer an den „APP Port“-Wert anpassen.

Wurden keine Befehlszeilenvariablen festgelegt, gelten für APP Server die folgenden Standardwerte:

- Zeitverzögerung zwischen zwei Verbindungsversuchen: 20 Sekunden
- Höchstzahl der Verbindungsversuche: 3 (3 mal 20 Sekunden)

- MAC-Adresse des APP-Server-PC: keine (Nullen)
- UPD-Port: 7001
- Broadcast-UDP-Port und Kommunikations-UDP-Port sind identisch
- APP Server erzwingt bei Ausführung eine Verbindung

Hinweis: Für den Zugriff auf das sichere entfernte Netzwerk wird ein Verbindungsprofil benötigt. Wird in der APP-Server-Zeile der Datei AUTOEXEC.BAT kein Verbindungsprofil angegeben, wird der Benutzer beim Systemstart aufgefordert, einen Verbindungsprofilnamen anzugeben.

So gibt der Befehl

```
C:\ASCEND\APPSRVDS.EXE /Chicago /t20 /p7005
```

z. B. an, daß ein Verbindungsprofil namens „Chicago“ verwendet, zwischen den einzelnen Verbindungsversuchen 20 Sekunden gewartet und für die Kommunikation mit der Pipeline die UDP-Port-Nummer 7005 zugewiesen werden soll.

Der Befehl

```
C:\ASCEND\appsrvDS.exe /Chicago /m00805110C7A44 /p7523 /t65 /
b7112
```

gibt als Name des Verbindungsprofils „Chicago“ an, legt als MAC-Adresse des APP-Server-PC 00805110C7A44 fest, weist für die Kommunikation mit der Pipeline die UDP-Portnummer 7523 zu, stellt eine Verzögerung von 65 Sekunden zwischen zwei Verbindungsversuchen ein und gibt an, daß Broadcast-Meldungen (zur Initiierung eines Rufes) den Port 7112 verwenden sollen.

Installation und Einsatz der Windows-Versionen von APP Server

Die Benutzeroberfläche ist für alle Windows-Versionen von APP Server gleich. Die Arbeitsweise und Installation unterscheiden sich jedoch.

Arbeiten mit den Windows-Versionen von APP Server

Für die Arbeit mit einer der Windows-Versionen des Dienstprogramms gelten die folgenden Schritte:

1 Starten Sie, falls noch nicht geschehen, APP Server durch Klicken auf „Services“ in der Systemsteuerung.

Es erscheint das folgende Dialogfeld:

2 Klicken Sie auf „Connect“.

Es erscheint ein Dialogfeld, in dem Sie verschiedene Einstellungen vornehmen können (siehe unten).

3 Geben Sie den Namen des Verbindungsprofils ein, mit dem Sie sich beim entfernten Netzwerk anmelden.

4 Geben Sie Ihren Benutzernamen ein.

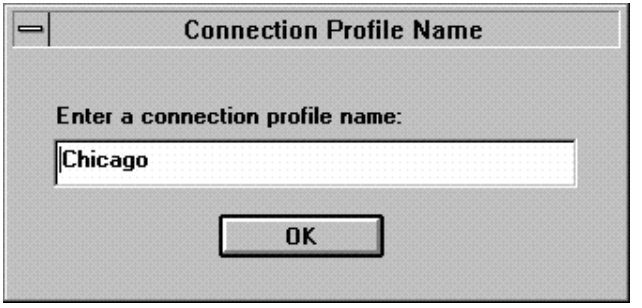
Der von Ihnen eingegebene Name darf nicht länger als 32 Zeichen sein. Er darf keine Leerzeichen enthalten.

5 Klicken Sie auf „OK“.

Nach Aushandlung der Sitzungsbedingungen gibt der entfernte ACE- bzw. SAFEWORD-Server eine Kennwortabfrage zurück, die in einem eigenen Dialogfeld erscheint. Der Benutzer hat 60 Sekunden Zeit, das aktuelle Kennwort von seiner Sicherheitskarte abzulesen und es fehlerfrei einzugeben.

6 Geben Sie das aktuelle Kennwort ein, und klicken Sie dann auf „OK“.

7 Zum Abmelden vom entfernten Netzwerk ist auf „Disconnect“ zu klicken. Es erscheint das folgende Dialogfeld:



8 Geben Sie den Namen des Verbindungsprofils ein, das die Einstellungen für Ihre Verbindung mit dem entfernten Netzwerk enthält. Klicken Sie dann auf „OK“.

Installieren der Windows 3.1-Version von APP Server

Zur Installation von APP Server auf einem Windows 3.1-System ist wie folgt vorzugehen:

1 Erstellen Sie im Stammverzeichnis ein Verzeichnis mit dem Namen \ASCEND.

2 Kopieren Sie die Datei APPSRV31.EXE in dieses Verzeichnis.

3 Wenn die Datei APPSRVR.INI bereits existiert, kopieren Sie sie ebenfalls in das Verzeichnis.

Siehe „Festlegen von Banner-Text für die Kennwort-Eingabeaufforderung“ auf Seite 9-32.

4 Kopieren Sie die Datei CTL3D.DLL in das Verzeichnis WINDOWS\SYSTEM.

Wir empfehlen, APP Server in die Programmgruppe „Autostart“ aufzunehmen. Voraussetzung dafür ist, daß das Netzwerk, einschließlich WINSOCK, als Teil eines normalen Systemstarts gestartet wird.

Um ein Programmsymbol zu erstellen und APP Server in die Programmgruppe „Autostart“ aufzunehmen, sind die folgenden Schritte auszuführen:

1 Erstellen Sie im Programm-Manager eine neue Programmgruppe.
Wählen Sie „Datei > Neu > Programmgruppe“, und geben Sie „Ascend“ ein.

2 Erstellen Sie ein Symbol für APPSRV31.EXE im Programm-Manager.
Wählen Sie dazu „Datei > Neu > Programm“.

3 Um APP Server starten zu lassen, sobald Windows gestartet wird, muß sich das APPSRV31.EXE-Symbol in der Programmgruppe „Autostart“ befinden.
Wenn APP Server nicht automatisch gestartet werden soll, können Sie das Dienstprogramm manuell starten, indem Sie auf sein Symbol doppelklicken.

4 Führen Sie einen Neustart durch.

Hinweise zur Arbeit mit APP Server unter Windows finden Sie im Abschnitt „Arbeiten mit den Windows-Versionen von APP Server“ auf Seite 9-38.

Installieren der Windows 95-Version von APP Server

Zur Installation von APP Server auf einem Windows 95-System ist wie folgt vorzugehen:

1 Kopieren Sie die Datei XAS-W95.EXE in ein temporäres Verzeichnis.
XAS-W95.EXE ist eine sich selbst dekomprimierende ZIP-Datei.

2 Starten Sie die Datei von der DOS-Eingabeaufforderung aus.
Sie entfaltet sich zu mehreren Dateien, unter denen sich auch das Setup-Programm für Windows 95 befindet.

3 Starten Sie das Setup-Programm in diesem Verzeichnis mit Hilfe des Start-Menüs.

4 Befolgen Sie die Anweisungen auf dem Bildschirm, und geben Sie ein Zielverzeichnis für die Installation der Windows 95-Version von APP Server an.

Die Windows 95-Version von APP Server startet automatisch, sobald das System erneut hochgefahren wird. Sie können APP Server während einer Sitzung zwar schließen, aber das Programm wird beim nächsten Systemstart erneut gestartet.

Soll APP Server permanent entfernt oder deaktiviert werden, müssen Sie in der Registrierung von Windows 95 den Schlüssel löschen, der auf APPSRV95.EXE weist.

Hinweise zur Arbeit mit APP Server unter Windows finden Sie im Abschnitt „Arbeiten mit den Windows-Versionen von APP Server“ auf Seite 9-38.

Installieren der Windows NT-Version von APP Server

Zur Installation von APP Server auf einem Windows NT-System ist wie folgt vorzugehen:

1 Kopieren Sie die Datei XAS-NT.EXE in ein temporäres Verzeichnis.
XAS-NT.EXE ist eine sich selbst dekomprimierende ZIP-Datei.

2 Starten Sie die Datei von der DOS-Eingabeaufforderung aus.
Sie entfaltet sich zu mehreren Dateien, unter denen sich auch das Setup-Programm für Windows NT befindet.

3 Starten Sie das Setup-Programm in diesem Verzeichnis.

4 Befolgen Sie die Anweisungen auf dem Bildschirm, und geben Sie ein Zielverzeichnis für die Installation der Windows NT-Version von APP Server an.

Die Windows NT-Version von APP Server startet automatisch, sobald das System erneut hochgefahren wird. Sie können APP Server während einer Sitzung zwar schließen, aber das Programm wird beim nächsten Systemstart erneut gestartet.

Während der Installation werden drei Symbole zur Verfügung gestellt, mit denen Sie APP Server vorübergehend deaktivieren, den Betrieb des Programms manuell steuern oder es aus dem System entfernen können:

- Symbol „Activate Service“
  Wenn Sie auf das Symbol „Activate Service“ klicken, wird der Dienst gestoppt (falls bereits aktiv) und dann neu gestartet oder aktiviert.
- Symbol „Remove Service“
  Wenn Sie auf das Symbol „Remove Service“ klicken, wird der Dienst gestoppt (falls aktiv) und aus der Dienste-Datenbank entfernt. Er erscheint dann nicht mehr in der Liste der Dienste im Applet „Services“ in der Systemsteuerung.

- Symbol „Uninstall Service“

  Wenn Sie auf das Symbol „Uninstall Service“ klicken, werden die mit APP Server zusammenhängenden Dateien, Symbole, Programme, Gruppen und Einträge in der Registrierungsdatenbank vom System entfernt.

Hinweise zur Arbeit mit APP Server unter Windows finden Sie im Abschnitt „Arbeiten mit den Windows-Versionen von APP Server“ auf Seite 9-38.

Definieren von Filtern

10

Dieses Kapitel enthält die folgenden Abschnitte:

Ascend-Filter – Einführung

Mit Ascend-Filtern werden bestimmte Paketbedingungen definiert. Wenn ein Filter angewendet wird, überprüft die Pipeline jedes Paket daraufhin, ob es die definierten Filterkriterien erfüllt, und unternimmt dann die entsprechenden Schritte. Welche Schritte dies sind, hängt zum einen von den jeweiligen Filterkriterien und zum anderen von der Art der Anwendung des Filters ab.

Wenn kein Filter verwendet wird, werden alle Pakete standardmäßig weitergeleitet, und der Timer wird zurückgesetzt. (Mit Hilfe des „Idle“-Timers wird bestimmt, wann inaktive Sitzungen abgebrochen werden sollen.) Im Filter kann festgelegt werden, daß bestimmte Pakete nicht weitergeleitet werden, oder aber daß *alle* Pakete weitergeleitet werden, *außer* den im Filter angegebenen. Darüber hinaus kann im Filter festgelegt werden, daß die Pipeline nur ankommende Pakete oder nur abgehende Pakete oder aber beides überprüft.

- Datenfilter

  Wird ein Filter als Datenfilter verwendet, bestimmt er, abhängig von den jeweiligen Filterfestlegungen, welche Pakete im Datenstrom weitergeleitet und welche ausgesondert werden. Datenfilter werden häufig zur Wahrung der Netzwerksicherheit verwendet, können aber auch für andere Zwecke eingesetzt werden.

- Ruffilter

  Wird ein Filter als Ruffilter verwendet, wirkt er sich nicht darauf aus, welche Pakete über eine aktive Verbindung gesendet werden. In einem Ruffilter wird mit der „Weiterleitungsaktion“ festgelegt, welche Pakete entweder eine Verbindung initiieren oder aber den Timer für eine aufgebaute Verbindung zurücksetzen können. Ruffilter werden vor allem dazu eingesetzt, unnötige Verbindungen zu verhindern.

Hinweis: Es ist möglich, Pakete von mehr als einem Filter filtern zu lassen. Soll der Datenstrom an einer Schnittstelle sowohl von einem Daten- als auch von einem Ruffilter gefiltert werden, müssen die Pakete zuerst den Datenfilter passieren.

Datenfilter

Datenfilter werden häufig zur Wahrung der Sicherheit verwendet, können aber auch für jede andere Situation eingesetzt werden, in der die Pipeline nur bestimmte Pakete weiterleiten können soll. So können Sie zum Beispiel Datenfilter verwenden, um Pakete auszusondern, die an einen bestimmten Host adressiert sind, oder um zu verhindern, daß regelmäßige Broadcasts über das WAN gesendet werden. Auf der anderen Seite können Sie Datenfilter verwenden, um sicherzustellen, daß Unbefugte über das WAN keinen Zugang zu bestimmten Geräten an Ihrem Standort haben.

Datenfilter wirken sich nicht auf den „Idle“-Timer aus. Ein Datenfilter, der auf ein Verbindungsprofil angewendet wird, hat auch keine Auswirkungen auf den Antwortprozeß.

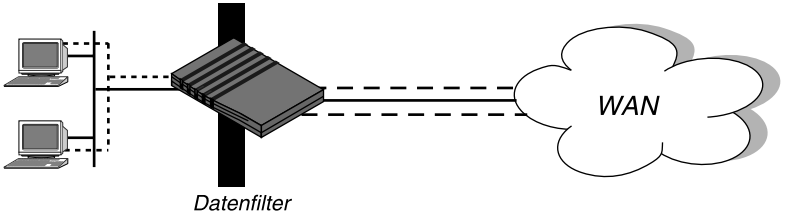


Abbildung 10-1: Datenfilter können bestimmte Pakete aussondern oder weiterleiten

Mit den folgenden Schritten legen Sie fest, welche Pakete eine WAN-Schnittstelle passieren dürfen:

1 Öffnen Sie ein „Connections“-Profil (bzw. das „Answer“-Profil).

2 Öffnen Sie das Untermenü „Session Options“.

3 Geben Sie die Nummer des Datenfilterprofils an.

Beispiel:

```
Data Filter=4
```

Wenn dieser Parameter den Standardwert 0 hat, findet keine Filterung statt. Die Nummern der definierten Filterprofile können Sie sich im Menü „Filters“ anzeigen lassen. Dabei muß nicht die gesamte Nummer, sondern nur der jeweils eindeutige Teil (z. B. 1, 2, 3, …) angegeben werden.

4 Schließen Sie das „Connections“-Profil (bzw. das „Answer“-Profil).

Filter, die auf ein Verbindungs- bzw. Antwortprofil angewendet werden, treten erst in Kraft, wenn die Verbindung aufgebaut wurde.

Mit den folgenden Schritten legen Sie fest, welche Pakete die Ethernet-Schnittstelle passieren dürfen:

1 Öffnen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

2 Öffnen Sie das Untermenü „Ether Options“.

3 Geben Sie die Nummer des Datenfilterprofils an.
Beispiel:

```
Data Filter=4
```

Wenn dieser Parameter den Standardwert 0 hat, findet keine Filterung statt. Die Nummern der definierten Filterprofile können Sie sich im Menü „Filters“ anzeigen lassen. Dabei muß nicht die gesamte Nummer, sondern nur der jeweils eindeutige Teil (z. B. 1, 2, 3, …) angegeben werden.

4 Schließen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

Filter, mit denen der Datenstrom an der Ethernet-Schnittstelle gefiltert werden soll, treten sofort in Kraft. Wenn Sie die Definition des Filterprofils ändern, gelten die neuen Filterkriterien, sobald Sie das Filterprofil speichern.

Im Abschnitt „Beispielfilter“ auf Seite 10-15 finden Sie ein Beispiel für einen Datenfilter.

Ruffilter

Ruffilter werden verwendet, um unnötige Verbindungen zu verhindern und um der Pipeline zu helfen, zwischen aktivem Verkehr und „Rauschen“ zu unterscheiden. Standardmäßig löst jeder Verkehr zu einem entfernten Standort einen Ruf zu diesem Standort aus und jeder Verkehr über eine aktive Verbindung setzt den „Idle“-Timer der Verbindung zurück.

Hinweis: Der „Idle“-Timer ist standardmäßig auf 120 Sekunden eingestellt. Ist eine Verbindung zwei Minuten lang inaktiv, sorgt der „Idle“-Timer dafür, daß die Pipeline die Verbindung beendet. Mit Ruffiltern werden Pakete festgelegt, die nicht als aktiver Verkehr über eine bestimmte Verbindung angesehen werden.

In Ruffiltern wird festgelegt, welche Pakete keine Rufe auslösen bzw. nicht den „Idle“-Timer zurücksetzen können. Sie haben jedoch keinen Einfluß darauf, welche Pakete über aktive Verbindungen gesendet oder empfangen werden.

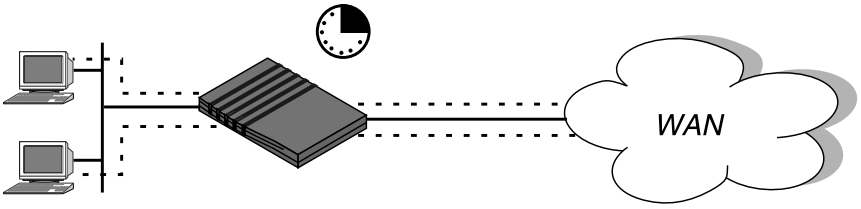


Abbildung 10-2: Ruffilter können verhindern, daß bestimmte Pakete den Timer zurücksetzen

Mit den folgenden Schritten können Sie einen Ruffilter zuweisen:

1 Öffnen Sie ein „Connections“-Profil (bzw. das „Answer“-Profil).

2 Öffnen Sie das Untermenü „Session Options“.

3 Geben Sie die Nummer des Ruffilterprofils an.

Beispiel:

```
Call Filter=5
```

Wenn dieser Parameter den Standardwert 0 hat, findet keine Filterung statt. Die Nummern der definierten Filterprofile können Sie sich im Menü „Filters“ anzeigen lassen. Dabei muß nicht die gesamte Nummer, sondern nur der jeweils eindeutige Teil (z. B. 1, 2, 3, …) angegeben werden.

4 Schließen Sie das „Connections“-Profil (bzw. das „Answer“-Profil).

Filter, mit denen der Verkehr über eine WAN-Schnittstelle gefiltert werden soll, treten erst in Kraft, wenn die Verbindung aufgebaut wurde.

Wenn der „Idle“-Timer zurückgesetzt werden soll, ist wie folgt vorzugehen:

1 Öffnen Sie ein „Connections“-Profil.

2 Öffnen Sie das Untermenü „Session Options“.

3 Geben Sie im Parameter „Idle“ an, wie viele Sekunden die Pipeline warten soll, bevor sie eine inaktive Verbindung beendet.

Beispiel:

```
Idle=15
```

Wenn dieser Parameter den Wert 0 (Null) hat, wird die inaktive Verbindung unbegrenzt aufrechterhalten.

Wenn Sie z. B. als Wert „15“ angeben, wird die inaktive Verbindung nach 15 Sekunden beendet.

4 Schließen Sie das „Connections“-Profil.

Vordefinierte Ruffilter

Die Pipeline enthält bei Auslieferung die folgenden vordefinierten Filterprofile:

- „IP Call“ – für IP-Verbindungen
- „NetWare Call“ – für IPX-Verbindungen
- „AppleTalk Call“ – für „gebridgte“ AppleTalk-Verbindungen

Bei diesen Filtern handelt es sich um grundlegende Ruffilter, mit denen der häufigste Routineverkehr in jeder Art von Paketstrom daran gehindert wird, Verbindungen zu initiieren bzw. aufrechtzuerhalten. Die internen Definitionen der vordefinierten Filter können Sie dem Abschnitt „Verwenden der vordefinierten Ruffilter“ auf Seite 10-27 entnehmen.

Hinweis: Informationen zu IPX-SAP-Filtern, mit denen festgelegt werden kann, welche NetWare-Dienste die Pipeline in ihre Dienstetabelle aufnimmt, entnehmen Sie bitte Kapitel 8, „Konfigurieren der Pipeline als IPX-Router“

Überblick über die Filterprofile

Abbildung 10-3 zeigt, wie die Filter in der Menüstruktur organisiert sind und welche Terminologie zur Beschreibung der einzelnen Teile eines Filters verwendet wird.

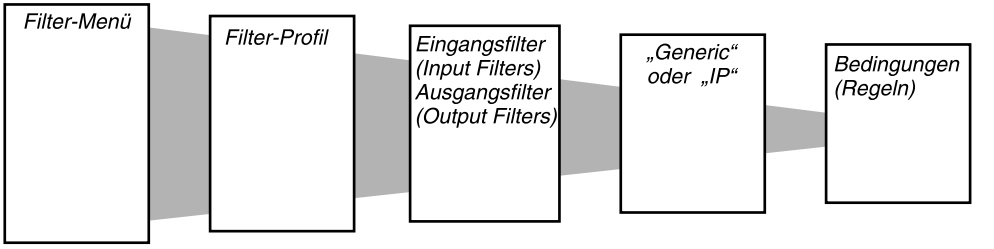


Abbildung 10-3: Filter-Terminologie

Hinweis: Bei den Menüs in Abbildung 10-3 handelt es sich um Untermenüs des Menüs „Filters“. Um einen Filter für eine Schnittstelle wirksam werden zu lassen, müssen Sie dessen Profilnummer angeben. Die Pipeline filtert den Verkehr dann entsprechend der in diesem Profil definierten Filterbedingungen.

- Menü „Filters“

  Das Menü „Filters“ enthält eine Liste mit numerierten Profilen. Bei der Festlegung, welcher Filter verwendet werden soll, braucht nur der eindeutige Teil der jeweiligen Filterprofilnummer des Filters angegeben zu werden (z. B. 1, 2, 3, …).

- Filterprofil

  Ein Filterprofil besteht aus einer Gruppe von definierten Filterkriterien.

- Eingangs- bzw. Ausgangsfilter

  Ganz oben in einem Filterprofil finden Sie die Untermenüs „Input Filters“ und „Output Filters“. Jedes dieser Untermenüs enthält eine Liste mit 12 Filtern. Die Kriterien, die Sie in diesen „In filters“ oder/und „Out filters“ festlegen, gelten für ankommende bzw. abgehende Pakete, wobei die Filter in der angegebenen Reihenfolge zugewiesen werden (1–12). Näheres dazu finden Sie im Abschnitt „Filtern von ankommenden und abgehenden Paketen“ auf Seite 10-8.

- Generische Filter bzw. IP-Filter

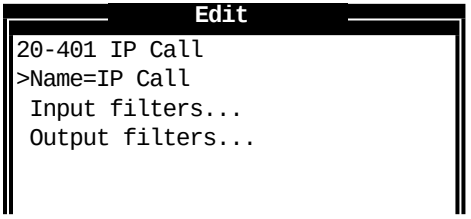
Jeder „In filter“ und „Out filter“ kann entweder den Typ „GENERIC“ oder aber den Typ „IP“ haben. Nach der Festlegung des Typs können Sie das entsprechende Untermenü öffnen und dort die Filterkriterien für das Weiterleiten bzw. Aussondern von Paketen definieren. Siehe dazu „Festlegen des Filtertyps und Aktivieren des Filters“ auf Seite 10-10.

- Filterkriterien

  Filterkriterien geben die Merkmale der Pakete an, die im Datenstrom untersucht werden sollen. Als generische Filterkriterien werden Orte und Werte angegeben, die in jedem Paket auftauchen können. Kriterien für IP-Filter sind IP-spezifische Paketmerkmale, wie z. B. die Adresse, die Maske und die Anschlußnummer (Portnummer).

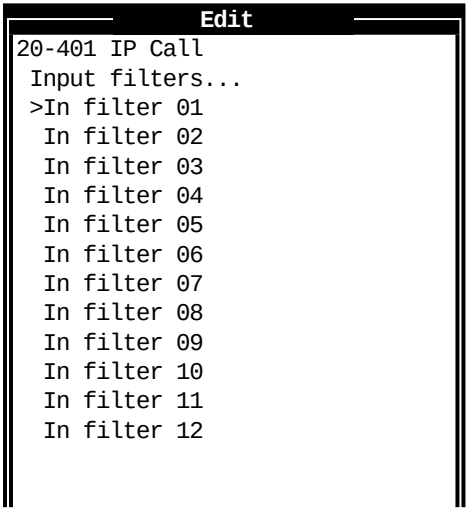
Filtern von ankommenden und abgehenden Paketen

In der obersten Ebene eines Filterprofils können Sie diesem einen Namen zuweisen und das Untermenü „Input Filters“ bzw. „Output Filters“ öffnen.



Bei der Verwendung von Eingangsfiltern (Input Filters) überprüft die Pipeline ankommende Pakete; Ausgangsfilter (Output Filters) dienen dagegen zur Überprüfung abgehender Pakete. Wird der Verkehr über die Ethernet-Schnittstelle mit einem Datenfilter gefiltert, sind davon Pakete aus dem Ethernet *zur* Pipeline bzw. Pakete von der Pipeline *in* das Ethernet betroffen. Daten- oder Ruffilter für eine WAN-Schnittstelle, die in einem Verbindungsprofil definiert wurde, gelten für Pakete von dieser WAN-Schnittstelle *zur* Pipeline bzw. von der Pipeline *zu* dieser Schnittstelle.

In einem Filterprofil können bis zu 12 „In filters“ und 12 „Out filters“ definiert werden. Diese Filter werden in der Reihenfolge angewendet, in der sie im Profil erscheinen (1–12).



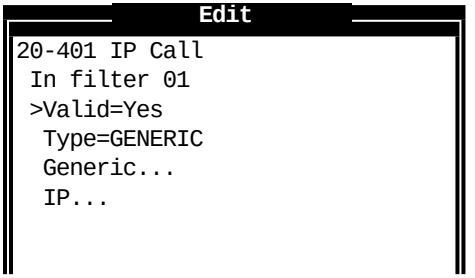
Standardmäßig werden Pakete weitergeleitet. Das heißt, daß Pakete, die keinem der im Filter definierten Kriterien entsprechen, wie gewöhnlich weitergeleitet werden.

Hinweis: Wurden nur Eingangsfilter definiert, werden die abgehenden Pakete standardmäßig alle weitergeleitet, bzw. alle abgehenden Pakete setzen den „Idle“-Timer zurück. Das gleiche gilt für die andere Richtung: Wurden nur Ausgangsfilter definiert, werden die ankommenden Pakete standardmäßig alle weitergeleitet, bzw. alle ankommenden Pakete setzen den „Idle“-Timer zurück.

Festlegen des Filtertyps und Aktivieren des Filters

Die von Ihnen definierten Eingangs- und Ausgangsfilter werden in der Reihenfolge angewendet, in der sie in der Liste erscheinen, wenn der Parameter „Valid“ für jeden der Filter auf „Yes“ gesetzt wurde. Hat der Parameter „Valid“ den Wert „No“, wird dieser Filter nicht angewendet.

Damit ein Eingangs- oder Ausgangsfilter wirksam wird, ist für den Parameter „Valid“ der Wert „Yes“ festzulegen und dann anzugeben, welcher Typ von Filterkriterien definiert werden soll („Generic“ oder „IP“).



In generischen Filtern werden Bits und Bytes in einem Paket definiert. Diese Filter gelten für alle Pakettypen, einschließlich TCP- und IP-Pakete. IP-Filter gelten dagegen nur für TCP-/IP-/UDP-Pakete.

Definieren der Kriterien für generische Filter

Wenn der Parameter „Type“ in einem Filter den Wert „GENERIC“ hat, werden generische Filterkriterien definiert. Table 10-1 zeigt die Filterkriterien für generische Filter.

Tabelle 10-1: Filterkriterien für generische Filter

Ort	Parameter mit Beispielwerten
Ethernet > Filters > *alle Profile* > Input filters > 01 bis 12 > Generic Ethernet > Filters > *alle Profile* > Output filters > 01 bis 12 > Generic (Filterprofil)	Forward=No Offset=14 Length=8 Mask=ffffffffffffffff Value=aaa030000000080f3 Compare=Equals More=No

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch.*

- „Forward“
  Der Parameter „Forward“ gibt an, was die Pipeline mit dem überprüften Paket machen soll, wenn es der Definition entspricht. Bei „Forward=Yes“ leitet sie das Paket weiter, während das Paket bei „Forward=No“ ausgesondert wird.
  Wenn der Filter als Datenfilter eingesetzt wird, wird mit „Forward“ festgelegt, welche Pakete gesendet und empfangen werden. Ist der Filter ein Rufilter, wird mit „Forward“ angegeben, welche Pakete eine Verbindung initiieren oder den „Idle“-Timer für eine bestehende Verbindung zurücksetzen können.
- „Offset“, „Length“, „Mask“ und „Value“
  Die Parameter „Offset“, „Length“, „Mask“ und „Value“ werden verwendet, um die exakte Position bestimmter Bytes innerhalb eines Pakets sowie den Wert dieser Bytes festzulegen.

- „Compare“

  Der Parameter „Compare“ gibt an, wie der Inhalt eines Pakets mit dem in diesem Filter angegebenen Wert verglichen werden soll. Nach Anwendung der Werte für „Offset“, „Length“ und „Mask“, um die entsprechende Position innerhalb eines Pakets zu erreichen, wird der Wert dieser Position mit dem Wert des Parameters „Value“ verglichen. Wurde für „Compare“ der Wert „Equals“ festgelegt (also der Standardwert beibehalten), wird der Filter angewendet, wenn die Paketdaten mit dem angegebenen Wert identisch sind. Hat „Compare“ den Wert „NotEquals“, wird der Filter angewendet, wenn die Paketdaten nicht identisch sind.

- „More“

  Der Parameter „More“ gibt an, ob der aktuelle Filter mit dem Filter verknüpft ist, der ihm unmittelbar folgt. Wenn „More=Yes“ festgelegt wurde, kann der Filter mehrere nicht zusammenhängende Bytes innerhalb eines Pakets überprüfen, indem er den aktuellen Filter mit dem nächsten verknüpft, so daß erst der nächste Filter angewendet wird, bevor eine Entscheidung für oder gegen die Weiterleitung getroffen wird. Eine Übereinstimmung liegt nur dann vor, wenn *beide* nicht zusammenhängenden Bytes die angegebenen Werte enthalten. Hat der Parameter „More“ den Wert „No“, erfolgt die Weiterleitungsentscheidung ausschließlich auf der Grundlage der Definition in diesem einen Filter.

Definieren der Kriterien für IP-Filter

Wurde für den Parameter „Type“ der Wert „IP“ festgelegt, können Sie Filterkriterien definieren, die nur für TCP-/IP-/UDP-Datenpakete (einschließlich „gebridgter“ Pakete) zutreffen.

Ein IP-Filter überprüft Ausgangsadressen, Zieladressen, den IP-Protokolltyp oder/und die Anschlußnummer. In Table 10-2 werden die Filterkriterien aufgeführt, die Sie in IP-Filtern festlegen können.

Tabelle 10-2: Filterkriterien für IP-Filter

Ort	**Parameter mit Beispielwerten**
Ethernet > Filters > *alle Profile* > Input filters > 01 bis 12 > Ip • Ethernet > Filters > *alle Profile* > Output filters > 01 bis 12 > Ip	Forward=Yes Src Mask=255.255.255.192 Src Adrs=192.100.40.128 Dst Mask=0.0.0.0 Dst Adrs=0.0.0.0 Protocol=0 Src Port Cmp=None Src Port #=N/A Dst Port Cmp=None Dst Port #=N/A TCP Estab=N/A

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch*.

- „Forward“

  Der Parameter „Forward“ gibt an, was die Pipeline mit dem überprüften Paket machen soll, wenn es der Definition entspricht. Bei „Forward=Yes“ leitet sie das Paket weiter, während das Paket bei „Forward=No“ ausgesondert wird.

  Wenn der Filter als Datenfilter eingesetzt wird, wird mit „Forward“ festgelegt, welche Pakete gesendet und empfangen werden. Ist der Filter ein Rufilter, wird mit „Forward“ angegeben, welche Pakete eine Verbindung initiieren oder den „Idle“-Timer für eine bestehende Verbindung zurücksetzen können.

- „Src Adrs“, „Src Mask“, „Dst Adrs“ und „Dst Mask“

  Die Parameter „Src Adrs“, „Src Mask“, „Dst Adrs“ und „Dst Mask“ geben den Wert der Felder für die Ausgangsadresse und -maske sowie die Zieladresse und -maske in einem Paket an. Mit Hilfe der Masken-Parameter („Src Mask“ und „Dst Mask“) lassen sich Teile der Ausgangs- bzw. Zieladresse ausblenden, wie z. B. die Hostnummer.

- „Protocol“

  Mit dem Parameter „Protocol“ wird ein TCP/IP-Protokoll angegeben. So steht z. B. der Wert „6“ für TCP-Pakete. In der folgenden Liste sind die am häufigsten benutzten Protokolle aufgeführt; die Protokollnummern sind jedoch nicht auf diese Liste beschränkt. Eine komplette Liste der Protokolle finden Sie im Abschnitt „Well-Known Port Numbers“ in RFC 1700, *Assigned Numbers*, von J. Reynolds und J. Postel, Oktober 1994.

  – 1 – ICMP
  – 5 – STREAM
  – 8 – EGP
  – 6 – TCP
  – 9 – alle privaten internen Gateway-Protokolle (z. B. IGRP von Cisco)
  – 11 – Network Voice Protocol
  – 17 – UDP
  – 20 – Host Monitoring Protocol
  – 22 – XNS IDP
  – 27 – Reliable Data Protocol
  – 28 – Internet Reliable Transport Protocol
  – 29 – ISO Transport Protocol Class 4
  – 30 – Bulk Data Transfer Protocol
  – 61 – alle hostinternen Protokolle
  – 89 – OSPF

- „Src Port #“, „Dst Port #“, „Src Port Cmp“ und „Dst Port Cmp“

  Mit den Parametern „Src Port #“, „Dst Port #“, „Src Port Cmp“ und „Dst Port Cmp“ wird angegeben, ob die Protokollports, mit denen die über TCP/IP laufenden Anwendungen gekennzeichnet werden, verglichen werden müssen. Als Vergleichswerte kommen Protokollnummern in Betracht, die kleiner als, größer als, gleich oder ungleich sind.

- „TCP Estab“

  Mit dem Parameter „TCP Estab“ kann festgelegt werden, daß Pakete nur dann die Filterkriterien erfüllen, wenn bereits eine TCP-Sitzung hergestellt wurde.

Beispielfilter

In diesem Abschnitt wird anhand von Beispielfiltern Schritt für Schritt die Definition von Filtern (generische Filter und IP-Filter) erläutert.

In diesem Abschnitt erfahren Sie, wie Sie bei der Erstellung von Filterprofilen vorzugehen haben. Zuweilen werden die vordefinierten Ruffilter modifiziert, um sie an die Art von Paketen anzupassen, die am jeweiligen Standort am häufigsten auftreten. Siehe dazu „Verwenden der vordefinierten Ruffilter“ auf Seite 10-27.

Beispiel für einen generischen Filter für AppleTalk-Broadcasts

In diesem Abschnitt wird gezeigt, wie Sie einen generischen Datenfilter definieren können, mit dem verhindert wird, daß lokaler AppleTalk-AEP- und NBP-Verkehr über das WAN gesendet wird. Im Datenfilter werden zunächst die Pakettypen festgelegt, die *nicht* gefiltert werden sollen:

- AARP-Pakete (AppleTalk Address Resolution Protocol)
- AppleTalk-Pakete, die nicht an die AppleTalk-Multicast-Adresse adressiert sind (wie z. B. normaler Verkehr im Zusammenhang mit einer AppleTalk-File-Server-Verbindung)
- sämtlicher nicht mit AppleTalk zusammenhängender Verkehr

Dann werden die Pakete definiert, die ausgesondert werden sollen:

- AEP-Pakete (AppleTalk Echo Protocol)
- NBP-Pakete (Name Binding Protocol)

Zum Definieren eines generischen Datenfilters ist wie folgt vorzugehen:

1 Markieren Sie ein unbenanntes Filterprofil im Menü „Filters“, und drücken Sie die Eingabetaste.

In diesem Beispiel wird das Filterprofil 20-403 gewählt.

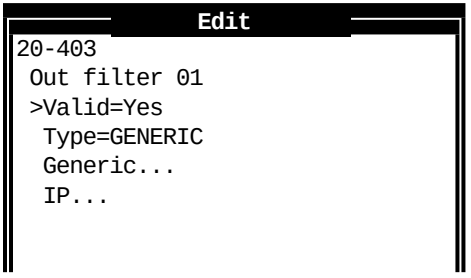
2 Weisen Sie dem Filterprofil einen Namen zu.

Beispiel:

```
Name=AppleTalk-Daten
```

3 Öffnen Sie das Untermenü „Output Filters“.

4 Öffnen Sie „Out filter 01“.



5 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „GENERIC“ fest. Öffnen Sie dann das Untermenü „Generic“, und nehmen Sie die folgenden Einstellungen vor:

```
Generic...
  >Forward=No
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa0300000080f3
   Compare=Equals
   More=No
```

Mit diesen Einstellungen wird eine Position innerhalb eines Pakets sowie der hexadezimale Wert festgelegt, den AARP-Pakete an dieser Position enthalten (Protokolltyp 0x80f3). Abgehende AARP-Pakete werden nicht weitergeleitet.

6 Schließen Sie „Out filter 01“, und öffnen Sie dann „Out filter 02“.

7 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „GENERIC“ fest. Öffnen Sie dann das Untermenü „Generic“, und nehmen Sie die folgenden Einstellungen vor:

```
Generic...
  >Forward=Yes
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa03080007809b
   Compare=NotEquals
   More=No
```

Diese Einstellungen dienen zur Definition des nicht mit AppleTalk zusammenhängenden Verkehrs (der Protokolltyp für AppleTalk ist 0x809b). Abgehende Pakete, die nicht AppleTalk-Pakete sind, werden weitergeleitet. Da bereits alle Pakete, die nicht AppleTalk-Pakete sind, weitergeleitet wurden, können die folgenden Filter davon ausgehen, daß es sich bei den von ihnen überprüften Paketen um AppleTalk-Pakete handelt.

8 Schließen Sie „Out filter 02“, und öffnen Sie dann „Out filter 03“.

9 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „GENERIC“ fest. Öffnen Sie dann das Untermenü „Generic“, und nehmen Sie die folgenden Einstellungen vor:

```
Generic...
  >Forward=Yes
   Offset=32
   Length=3
   Mask=ffffff0000000000
   Value=0404040000000000
   Compare=Equals
   More=No
```

Mit diesen Einstellungen werden AEP-Pakete gefiltert.

10 Schließen Sie „Out filter 03“, und öffnen Sie dann „Out filter 04“.

11 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „GENERIC“ fest. Öffnen Sie dann das Untermenü „Generic“, und nehmen Sie die folgenden Einstellungen vor:

```
Generic...
  >Forward=Yes
   Offset=32
   Length=6
   Mask=ffffffffffff0000
   Value=090007ffffff0000
   Compare=NotEquals
   More=No
```

Der AppleTalk-„Broadcast“-Verkehr verwendet eine Multicast-Adresse. In diesen Filterkriterien wird eine Multicast-Adresse angegeben. Alle AppleTalk-Pakete, die die Multicast-Adresse nicht verwenden, werden weitergeleitet.

12 Schließen Sie „Out filter 04“, und öffnen Sie dann „Out filter 05“.

13 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „GENERIC“ fest. Öffnen Sie dann das Untermenü „Generic“, und nehmen Sie die folgenden Einstellungen vor:

```
Generic...
  >Forward=Yes
   Offset=32
   Length=4
   Mask=ff00fff000000000
   Value=0200022000000000
   Compare=Equals
   More=Yes
```

In den Ausgangsfiltern 05 und 06 werden NBP-Abfrage-Pakete angegeben, wobei als Entitätsname ein „Joker“ verwendet wird. (NBP-Abfrage-Pakete werden von der Auswahl und anderen Anwendungen gesendet, die nach Entitäten in AppleTalk-Netzwerken suchen.)

14 Schließen Sie „Out filter 05“, und öffnen Sie dann „Out filter 06“.

15 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „GENERIC“ fest. Öffnen Sie dann das Untermenü „Generic“, und nehmen Sie die folgenden Einstellungen vor:

```
Generic...
  >Forward=Yes
   Offset=42
   Length=2
   Mask=ffff000000000000
   Value=013d000000000000
   Compare=Equals
   More=No
```

16 Schließen Sie „Out filter 06“, und öffnen Sie dann „Out filter 07“.

17 Legen Sie „Valid=Yes“ fest.

Um alles andere außer Kraft zu setzen, braucht für „Valid“ einfach nur „Yes“ festgelegt zu werden. Dies führt zu den folgenden Standardeinstellungen:

```
Generic...
  >Forward=No
   Offset=0
   Length=0
   Mask=0000000000000000
   Value=0000000000000000
   Compare=Equals
   More=No
```

18 Schließen Sie das Filterprofil.

Beispiel für einen IP-Filter zur Verhinderung des Adressen-Spoofing

In diesem Abschnitt wird die Definition eines IP-Datenfilters gezeigt, dessen Ziel es ist, die „Überlistung“ („Spoofing“) von lokalen IP-Adressen zu verhindern. Das IP-Adressen-Spoofing – nicht zu verwechseln mit dem an anderer Stelle beschriebenen Watchdog- oder DHCP-Spoofing – ist ein Verfahren, bei dem Benutzer von außerhalb des lokalen Netzwerks so tun, als wären sie Teil des lokalen Netzwerks, um unbefugterweise Zugriff auf das Netzwerk zu erlangen.

Im Filter werden zunächst Eingangsfilter definiert, die Pakete aussondern, deren Ausgangsadresse sich im lokalen IP-Netzwerk befindet oder die die Rückschleifadresse (127.0.0.0) haben. Die Aussage dieser Filter ist: „Wenn du ein ankommendes Paket siehst, das eine dieser Ausgangsadressen hat, sondere es aus.“ Mit dem dritten Eingangsfilter wird jede andere Ausgangsadresse festgelegt (0.0.0.0) und angegeben, das alles andere zum lokalen Netzwerk weitergeleitet werden soll.

Danach wird ein Ausgangsfilter definiert, dessen Aussage lautet: „Wenn ein abgehendes Paket eine Ausgangsadresse im lokalen Netzwerk hat, leite es weiter; alle anderen ankommenden Pakete sind auszusondern.“ Alle abgehenden Pakete, deren Ausgangsadresse nicht im lokalen Netzwerk liegt, werden also ausgesondert.

Hinweis: Dieses Beispiel geht von der lokalen IP-Netzwerkadresse 192.100.50.128 aus, wobei als Subnetzmaske 255.255.255.192 zum Einsatz kommt. Sie müssen bei der Definition eines Filterprofils natürlich Ihre eigene lokale IP-Adresse und Netzmaske verwenden.

Hinweis: Da die Pipeline nur 3 Filter unterstützt, modifiziert dieses Beispiel den vordefinierten IP-Ruffilter. Weitere Informationen zu den vordefinierten Filtern entnehmen Sie bitte dem Abschnitt „Verwenden der vordefinierten Ruffilter“ auf Seite 10-27.

Zum Definieren eines IP-Datenfilters ist wie folgt vorzugehen:

1 Markieren Sie ein unbenanntes Filterprofil im Menü „Filters“, und drücken Sie die Eingabetaste.
In diesem Beispiel wird das Filterprofil 20-401 gewählt.

```
Edit
20-400 Filters
 20-401 IP Call
 20-402 NetWare Call
 20-403 AppleTalk Call
```

2 Weisen Sie dem Filterprofil einen Namen zu.
Beispiel:
`Name=Kein Spoofing`

```
Edit
20-401
>Name=Kein Spoofing
 Input filters...
 Output filters...
```

3 Öffnen Sie das Untermenü „Input Filters“.

4 Öffnen Sie „In filter 01“.

```
Edit
20-401
 In filter 01
 >Valid=Yes
  Type=IP
  Generic...
  IP...
```

5 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „IP“ fest, und öffnen Sie dann das Untermenü „IP“.

6 Nehmen Sie die folgenden Einstellungen vor:

```
Ip...
>Forward=No
 Src Mask=255.255.255.192
 Src Adrs=192.100.50.128
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

Mit diesen Einstellungen wird in den Feldern „Src Mask“ und „Src Adrs“ die lokale Netzmaske und IP-Adresse festgelegt. Wenn ein ankommendes Paket eine lokale Adresse hat, wird es nicht über die Ethernet-Schnittstelle weitergeleitet.

7 Schließen Sie „In filter 01“, und öffnen Sie dann „In filter 02“.

8 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „IP“ fest, öffnen Sie dann das Untermenü „IP“, und nehmen Sie die folgenden Einstellungen vor:

```
Ip...
>Forward=No
 Src Mask=255.0.0.0
 Src Adrs=127.0.0.0
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

Mit diesen Einstellungen wird in den Feldern „Src Mask“ und „Src Adrs“ die Rückschleifadresse angegeben. Wenn ein ankommendes Paket diese Adresse hat, wird es nicht über die Ethernet-Schnittstelle weitergeleitet.

9 Schließen Sie „In filter 02“, und öffnen Sie dann „In filter 03“.

10 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „IP“ fest, öffnen Sie dann das Untermenü „IP“, und nehmen Sie die folgenden Einstellungen vor:

```
Ip...
>Forward=Yes
 Src Mask=0.0.0.0
 Src Adrs=0.0.0.0
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

Mit diesen Einstellungen wird jede andere Ausgangsadresse festgelegt (0.0.0.0). Wenn ein ankommendes Paket eine nicht zum lokalen Netzwerk gehörende Adresse hat, wird es nicht über die Ethernet-Schnittstelle weitergeleitet.

11 Schließen Sie „In filter 03“, und kehren Sie zur obersten Ebene des Filterprofils „Kein Spoofing“ zurück.

12 Öffnen Sie das Untermenü „Output Filters“, und öffnen Sie „Out filter 01“.

13 Legen Sie für „Valid“ den Wert „Yes“ und für „Type“ den Wert „IP“ fest, öffnen Sie dann das Untermenü „IP“, und nehmen Sie die folgenden Einstellungen vor:

```
Ip...
>Forward=Yes
 Src Mask=255.255.255.192
 Src Adrs=192.100.40.128
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

Mit diesen Einstellungen wird in den Feldern „Src Mask“ und „Src Adrs“ die lokale Netzmaske und IP-Adresse festgelegt. Wenn ein abgehendes Paket eine lokale Adresse hat, wird es nicht über die Ethernet-Schnittstelle weitergeleitet.

14 Schließen Sie das Filterprofil.

Beispiel für einen IP-Filter für komplexere Sicherheitsvorkehrungen

In diesem Abschnitt wird ein IP-Datenfilter beschrieben, der einige der Punkte illustriert, die beim Schreiben eigener IP-Filter u. U. zu beachten sind. Der Beispielfilter weist nicht auf Feineinstellungen der Netzwerksicherheit hin. Er kann z. B. als Ausgangspunkt für die Einrichtung von Sicherheitsmaßnahmen verwendet werden, die an Ihre eigenen Bedürfnisse angepaßt sind.

In diesem Beispiel unterstützt das lokale Netzwerk einen Web-Server, und der Administrator muß Benutzern die Möglichkeit geben, sich über die IP-Adresse des Servers einzuwählen, während der Zugriff auf alle anderen Hosts im lokalen Netzwerk über Wählverbindungen verweigert werden soll. Viele lokale IP-Hosts müssen jedoch in der Lage sein, abgehende Rufe zu starten, um z. B. auf das Internet zuzugreifen und Anwendungen auf IP-Basis zu nutzen, wie z. B. Telnet oder FTP. Das heißt, daß deren Antwort-

pakete entsprechend zum Ausgangshost geleitet werden müssen. In diesem Beispiel lautet die IP-Adresse des Web-Servers 192.9.250.5.

Dieser Filter würde als Datenfilter in Verbindungsprofilen angewendet werden.

```
In filter 01...Ip...Forward=Yes
In filter 01...Ip...Src Mask=0.0.0.0
In filter 01...Ip...Src Adrs=0.0.0.0
In filter 01...Ip...Dst Mask=255.255.255.255
In filter 01...Ip...Dst Adrs=192.9.250.5
In filter 01...Ip...Protocol=6
In filter 01...Ip...Src Port Cmp=None
In filter 01...Ip...Src Port #=N/A
In filter 01...Ip...Dst Port Cmp=Eql
In filter 01...Ip...Dst Port #=80
In filter 01....Ip....TCP Estab=No

In filter 02...Ip...Forward=Yes
In filter 02...Ip...Src Mask=0.0.0.0
In filter 02...Ip...Src Adrs=0.0.0.0
In filter 02...Ip...Dst Mask=0.0.0.0
In filter 02...Ip...Dst Adrs=0.0.0.0
In filter 02...Ip...Protocol=6
In filter 02...Ip...Src Port Cmp=None
In filter 02...Ip...Src Port #=N/A
In filter 02...Ip...Dst Port Cmp=Gtr
In filter 02...Ip...Dst Port #=1023
In filter 02....Ip....TCP Estab=No

In filter 03...Ip...Forward=Yes
In filter 03...Ip...Src Mask=0.0.0.0
In filter 03...Ip...Src Adrs=0.0.0.0
In filter 03...Ip...Dst Mask=0.0.0.0
In filter 03...Ip...Dst Adrs=0.0.0.0
In filter 03...Ip...Protocol=17
In filter 03...Ip...Src Port Cmp=None
In filter 03...Ip...Src Port #=N/A
In filter 03...Ip...Dst Port Cmp=Gtr
In filter 03...Ip...Dst Port #=1023
In filter 03....Ip....TCP Estab=No
```

```
In filter 04...Ip...Forward=Yes
In filter 04...Ip...Src Mask=0.0.0.0
In filter 04...Ip...Src Adrs=0.0.0.0
In filter 04...Ip...Dst Mask=0.0.0.0
In filter 04...Ip...Dst Adrs=0.0.0.0
In filter 04...Ip...Protocol=1
In filter 04...Ip...Src Port Cmp=None
In filter 04...Ip...Src Port #=N/A
In filter 04...Ip...Dst Port Cmp=None
In filter 04...Ip...Dst Port #=N/A
In filter 04....Ip....TCP Estab=No
```

Im ersten Eingangsfilter („In filter 01“) wird die IP-Adresse des Web-Servers als Ziel angegeben und festgelegt, daß alle ankommenden IP-Pakete mit dieser Zieladresse weitergeleitet werden.

Im zweiten Eingangsfilter („In filter 02“) wird angegeben, daß TCP-Pakete (Protocol=6) *von* jeder Adresse und *für* jede Adresse weitergeleitet werden sollen, wenn die Nummer des Zielports größer als die des Ausgangsports ist. So gehen z. B. Telnet-Anforderungen über den Port 23 ab, und Antworten werden über einen zufällig festgelegten Port mit einer Portnummer größer als 1023 empfangen. Mit diesem Filter werden also Pakete definiert, die zurückkommen, um auf die Telnet-Anforderungen eines Benutzers (oder andere Anfragen, bei denen TCP verwendet wird) für einen entfernten Host zu reagieren.

Im dritten Eingangsfilter („In filter 03“) werden UDP-Pakete (Protocol=17) mit genau derselben Situation angegeben wie oben für Telnet beschrieben. Wenn zum Beispiel ein RIP-Paket als ein UDP-Paket zum Zielport 520 gesendet wird, wird die Antwort auf diese Anforderung auch an einen zufällig festgelegten Port mit einer Portnummer größer als 1023 gesendet.

Der vierte Eingangsfilter („In filter 04“) schließlich spezifiziert unbegrenzte Pings und Traceroutes. ICMP verwendet keine Ports wie TCP und UDP, so daß ein Portvergleich nicht erforderlich ist.

Verwenden der vordefinierten Ruffilter

Die Pipeline wird mit drei vordefinierten Filterprofilen ausgeliefert – für jede der am häufigsten benutzten Protokollgruppen eines:

- „IP Call“ – für IP-Verbindungen
- „NetWare Call“ – für IPX-Verbindungen
- „AppleTalk Call“ – für „gebridgte“ AppleTalk-Verbindungen

Diese vordefinierten Filter sind als Ruffilter gedacht, mit deren Hilfe die Verbindungskosten möglichst gering gehalten werden sollen. Sie stellen eine Grundlage dar, auf der Sie die Ihrer Umgebung entsprechenden Feineinstellungen für die Behandlung des Routineverkehrs in Ihrem Netzwerk durch die Pipeline vornehmen können.

Hinweis: Sie können die vordefinierten Filterprofile modifizieren, um Sie für die Paketarten anzupassen, die am häufigsten in Ihrem Netzwerk auftreten, und bei denen verhindert werden soll, daß sie Verbindungen initiieren oder aufrechterhalten.

NetWare-Ruffilter („NetWare Call“)

Der vordefinierte NetWare-Ruffilter („NetWare Call“) soll SAP-Pakete (Service Advertising Protocol), die ihren Ursprung im lokalen IPX -Netzwerk haben, daran hindern, den „Idle“-Timer zurückzusetzen oder einen Ruf zu initiieren.

NetWare-Server senden alle 60 Sekunden SAP-Broadcast-Pakete, um zu gewährleisten, daß alle Router und Bridges die verfügbaren Dienste kennen. Um zu verhindern, daß diese Pakete eine Verbindung unnötigerweise aufrechterhalten, können Sie den vordefinierten NetWare-Ruffilter im Untermenü „Session Options“ der Verbindungsprofile einsetzen, in denen das IPX-Routing aktiviert ist.

Der vordefinierte NetWare-Ruffilter enthält sechs Ausgangsfilter („Out filters“), die abgehende SAP-Pakete identifizieren und die Pakete davon abhalten, den „Idle“-Timer zurückzusetzen oder einen Ruf zu initiieren.

```
Out filter 01...Generic...Forward=No
Out filter 01...Generic...Offset=14
Out filter 01...Generic...Length=3
Out filter 01...Generic...Mask=ffffff000000000000
Out filter 01...Generic...Value=e0e0030000000000
Out filter 01...Generic...Compare=Equals
Out filter 01....Generic....More=Yes

Out filter 02...Generic...Forward=No
Out filter 02...Generic...Offset=27
Out filter 02...Generic...Length=8
Out filter 02...Generic...Mask=ffffffffffff
Out filter 02...Generic...Value=fffffffffff0452
Out filter 02...Generic...Compare=Equals
Out filter 02....Generic....More=Yes

Out filter 03...Generic...Forward=No
Out filter 03...Generic...Offset=47
Out filter 03...Generic...Length=2
Out filter 03...Generic...Mask=ffff000000000000
Out filter 03...Generic...Value=0002000000000000
Out filter 03...Generic...Compare=Equals
Out filter 03....Generic....More=No

Out filter 04...Generic...Forward=No
Out filter 04...Generic...Offset=12
Out filter 04...Generic...Length=4
Out filter 04...Generic...Mask=fc00ffff00000000
Out filter 04...Generic...Value=0000ffff00000000
Out filter 04...Generic...Compare=Equals
Out filter 04....Generic....More=Yes

Out filter 05...Generic...Forward=No
Out filter 05...Generic...Offset=24
Out filter 05...Generic...Length=8
Out filter 05...Generic...Mask=ffffffffffffff
Out filter 05...Generic...Value=fffffffffff0452
Out filter 05...Generic...Compare=Equals
Out filter 05....Generic....More=Yes
```

```
Out filter 06...Generic...Forward=No
Out filter 06...Generic...Offset=44
Out filter 06...Generic...Length=2
Out filter 06...Generic...Mask=ffff000000000000
Out filter 06...Generic...Value=0002000000000000
Out filter 06...Generic...Compare=Equals
Out filter 06....Generic....More=No
```

Ausweiten des vordefinierten NetWare-Filters auf RIP-Pakete

Um den NetWare-Ruffilter so zu erweitern, daß er auch IPX-RIP-Pakete davon abhält, den „Idle“-Timer zurücksetzen oder einen Ruf zu initiieren, können Sie die folgenden zusätzlichen Ausgangsfilter („Out filters“) definieren:

```
Out filter 07...Generic...Forward=No
Out filter 07...Generic...Offset=0
Out filter 07...Generic...Length=6
Out filter 07...Generic...Mask=ffffffffffff0000
Out filter 07...Generic...Value=ffffffffffff0000
Out filter 07...Generic...Compare=Equals
Out filter 07....Generic....More=Yes

Out filter 08...Generic...Forward=No
Out filter 08...Generic...Offset=24
Out filter 08...Generic...Length=8
Out filter 08...Generic...Mask=ffffffffffff
Out filter 08...Generic...Value=ffffffffffff0453
Out filter 08...Generic...Compare=Equals
Out filter 08....Generic....More=No

Out filter 09...Generic...Forward=No
Out filter 09...Generic...Offset=0
Out filter 09...Generic...Length=6
Out filter 09...Generic...Mask=ffffffffffff0000
Out filter 09...Generic...Value=ffffffffffff0000
Out filter 09...Generic...Compare=Equals
Out filter 09....Generic....More=Yes

Out filter 10...Generic...Forward=No
Out filter 10...Generic...Offset=27
```

```
Out filter 10...Generic...Length=8
Out filter 10...Generic...Mask=ffffffffffffffff
Out filter 10...Generic...Value=fffffffffff0453
Out filter 10...Generic...Compare=Equals
Out filter 10....Generic....More=No

Out filter 11...Generic...Forward=Yes
Out filter 11...Generic...Offset=0
Out filter 11...Generic...Length=0
Out filter 11...Generic...Mask=0000000000000000
Out filter 11...Generic...Value=0000000000000000
Out filter 10...Generic...Compare=Equals
Out filter 11....Generic....More=No
```

Definieren eines SNEP-Datenfilters für die Ethernet-Schnittstelle

Der Kopierschutzmechanismus von NetWare arbeitet mit SNEP-Paketen (Serialization Number Exchange Protocol), die von allen Servern im Netzwerk gesendet oder empfangen werden. SNEP-Pakete treten als Anforderungs-/Antwort-Paare zwischen Servern auf. Wenn auf beiden Seiten des WAN NetWare-Server unterstützt werden, kann dieser Austausch von Paketen eine IPX-Verbindung unnötigerweise aufrechterhalten.

Der folgende Beispiel-SNEP-Filter ist für den Einsatz als Datenfilter an der Ethernet-Schnittstelle gedacht. Um einen SNEP-Datenfilter für die Ethernet-Schnittstelle der Pipeline zu erstellen, müssen Sie ein neues Filterprofil anlegen und die folgenden Eingangsfilter („In filter“) definieren:

```
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=30
In filter 01...Generic...Length=2
In filter 01...Generic...Mask=ffff000000000000
In filter 01...Generic...Value=0457000000000000
In filter 01...Generic...Compare=Equals
In filter 01....Generic....More=No

In filter 02...Generic...Forward=No
In filter 02...Generic...Offset=33
In filter 02...Generic...Length=2
In filter 02...Generic...Mask=ffff000000000000
```

```
In filter 02...Generic...Value=0457000000000000
In filter 02...Generic...Compare=Equals
In filter 02....Generic....More=No

In filter 03...Generic...Forward=Yes
In filter 03...Generic...Offset=0
In filter 03...Generic...Length=0
In filter 03...Generic...Mask=0000000000000000
In filter 03...Generic...Value=0000000000000000
In filter 03...Generic...Compare=Equals
In filter 03....Generic....More=No
```

Wenn im NetWare-Ruffilter genügend Ausgangsfilter zur Verfügung stehen, (zum Beispiel, wenn der Filter nicht auch auf RIP-Pakete ausgeweitet wird, wie in „Ausweiten des vordefinierten NetWare-Filters auf RIP-Pakete“ auf Seite 10-29 beschrieben), oder wenn Sie mit NetWare 4.0 oder höher arbeiten und die vordefinierten SAP-Filter nicht benötigen, können Sie statt dessen festlegen, daß diese SNEP-Filter als Ausgangsfilter im Ruffilter verwendet werden sollen.

IP-Ruffilter („IP Call“)

Der vordefinierte IP-Ruffilter („IP Call“) hält ankommende Pakete davon ab, den „Idle“-Timer zurückzusetzen. Abgehende Pakete werden dagegen nicht davon abgehalten, den Timer zurückzusetzen oder einen Ruf zu initiieren.

Der IP-Ruffilter enthält einen Eingangsfilter („In filter“), der alle ankommenden Pakete definiert, und einen Ausgangsfilter („Out filter“), der alle abgehenden Pakete definiert (alle abgehenden Pakete, die für das im Verbindungsprofil, in dem der Filter angewendet werden soll, angegebene entfernte Netzwerk bestimmt sind).

```
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=0
In filter 01...Generic...Length=0
In filter 01...Generic...Mask=0000000000000000000
In filter 01...Generic...Value=0000000000000000
In filter 01...Generic...Compare=Equals
In filter 01....Generic....More=No
```

```
Out filter 01...Generic...Forward=Yes
Out filter 01...Generic...Offset=0
Out filter 01...Generic...Length=0
Out filter 01...Generic...Mask=000000000000000000
Out filter 01...Generic...Value=0000000000000000
Out filter 01...Generic...Compare=Equals
Out filter 01....Generic....More=No
```

AppleTalk-Ruffilter („AppleTalk Call“)

Der AppleTalk-Ruffilter („AppleTalk Call“) weist die Pipeline an, je nach der AppleTalk-Aktivität im LAN einen Ruf zu initiieren und den „Idle“-Timer zurückzusetzen, ankommenden Paketen oder AEP-Paketen (AppleTalk Echo) dieses aber zu verwehren. Er enthält einen Eingangsfilter („In filter“) und fünf Ausgangsfilter („Out filter“).

Der Eingangsfilter verhindert, daß ankommende Pakete den „Idle“-Timer zurücksetzen oder einen Ruf initiieren. In den ersten beiden Ausgangsfiltern wird das AppleTalk Phase II AEP-Protokoll angegeben, während in den nächsten beiden Ausgangsfiltern das AppleTalk Phase I AEP-Protokoll verwendet wird. Da der Parameter „More“ im ersten der beiden Filterpaare den Wert „Yes“ und im zweiten den Wert „No“ hat, muß ein Paket die Kriterien in beiden Filtern erfüllen, damit es den Filterbedingungen entspricht. Der letzte Ausgangsfilter weist die Pipeline an, allen anderen abgehenden Paketen zu erlauben, den „Idle“-Timer zurückzusetzen bzw. einen Ruf zu initiieren.

```
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=0
In filter 01...Generic...Length=0
In filter 01...Generic...Mask=000000000000000000
In filter 01...Generic...Value=0000000000000000
In filter 01...Generic...Compare=Equals
In filter 01....Generic....More=No

Out filter 01...Generic...Forward=No
Out filter 01...Generic...Offset=14
Out filter 01...Generic...Length=8
Out filter 01...Generic...Mask=ffffff000000ffff
Out filter 01...Generic...Value=aaaa03000000809b
```

```
Out filter 01...Generic...Compare=Equals
Out filter 01....Generic....More=Yes

Out filter 02...Generic...Forward=No
Out filter 02...Generic...Offset=33
Out filter 02...Generic...Length=3
Out filter 02...Generic...Mask=ffffff0000000000
Out filter 02...Generic...Value=0404040000000000
Out filter 02...Generic...Compare=Equals
Out filter 02....Generic....More=No

Out filter 03...Generic...Forward=No
Out filter 03...Generic...Offset=12
Out filter 03...Generic...Length=2
Out filter 03...Generic...Mask=ffff000000000000
Out filter 03...Generic...Value=809b000000000000
Out filter 03...Generic...Compare=Equals
Out filter 03....Generic....More=Yes

Out filter 04...Generic...Forward=No
Out filter 04...Generic...Offset=24
Out filter 04...Generic...Length=3
Out filter 04...Generic...Mask=ffffff0000000000
Out filter 04...Generic...Value=0404040000000000
Out filter 04...Generic...Compare=Equals
Out filter 04....Generic....More=No

Out filter 05...Generic...Forward=yes
Out filter 05...Generic...Offset=0
Out filter 05...Generic...Length=0
Out filter 05...Generic...Mask=0000000000000000
Out filter 05...Generic...Value=0000000000000000
Out filter 05...Generic...Compare=Equals
Out filter 05....Generic....More=No
```

Systemadministration

11

Dieses Kapitel enthält die folgenden Abschnitte:

Ascend-Systemadministration – Einführung

Diese Einführung gibt einen Überblick über die administrativen Funktionen der Pipeline und enthält Hinweise, wo Sie weitere Informationen erhalten können.

Administrationsfunktionen in der VT100-Schnittstelle

Die VT100-Schnittstelle der Pipeline bietet Ihnen die folgenden administrativen Funktionen:

- Sicherheitsprofile

  Die Pipeline kann mit Hilfe von Kennwörtern vor dem Zugriff durch Unbefugte geschützt werden. Siehe dazu „Aktivieren der Administrationsprivilegien“ auf Seite 11-4. Nähere Informationen zu den Sicherheitsprofilen finden Sie im Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

- Befehle zur Systemadministration

  Die Pipeline verfügt über Befehle zum Neustarten des Geräts, Speichern bzw. Wiederherstellen von Konfigurationsinformationen und zur Verwendung anderer administrativer Funktionen. Die Systemsoftware der Pipeline kann durch den Kunden vor Ort aktualisiert werden, ohne daß dazu die Einheit geöffnet oder Speicherchips ausgetauscht werden müssen. Bei diesem Vorgang werden auch Befehle zum Konfigurationsmanagement verwendet. Siehe dazu „Ausführen von Systemadministrations-Operationen“ auf Seite 11-22.

- DO-Befehle

  Durch Drücken der Tastenkombination Strg-D in der VT100-Schnittstelle öffnen Sie das DO-Menü, das Befehle zur Änderung der Sicherheitsebenen in der Pipeline und zum manuellen Wählen bzw. Beenden von Rufen enthält. Wenn Sie die Sicherheitsebene „Full Access“ (oder eine andere entsprechende Sicherheitsebene) aktiviert haben, können Sie alle DO-Befehle sowie alle anderen administrativen Operationen ausführen.

- Befehlszeilen-Schnittstelle des Terminal-Servers

  Die Befehlszeilen-Schnittstelle der Pipeline enthält Befehle zum Testen von Verbindungen, Überprüfen der Routing-Tabellen und anderer Konfigurationsparameter sowie zum Konfigurieren von entfernten Ascend-Einheiten über das WAN. Viele dieser Befehle haben auch mit der

Systemadministration zu tun. Siehe „Die Terminal-Server-Befehlszeile“ auf Seite 11-31.

- Statusfenster

  Die Statusfenster in der VT100-Schnittstelle bieten Informationen darüber, was gegenwärtig in der Pipeline vor sich geht. So werden z. B. in einem Statusfenster bis zu 31 der Systemereignisse, die seit dem Einschalten der Pipeline aufgetreten sind, sowie statistische Angaben über die gegenwärtig aktive Sitzung angezeigt. Mit Hilfe der Statusfenster können darüber hinaus auch einige DO-Befehle, wie z. B. das Beenden einer aktiven Verbindung, ausgeführt werden.

- Interaktion mit dem Syslog-Dämonen zur Erstellung von ASCII-Protokolldateien

  Wenn auf einem Windows- oder UNIX-Host im lokalen Netzwerk der Syslog-Dämon läuft, können Sie die Pipeline so konfigurieren, daß sie Protokollmeldungen in eine ASCII-Datei auf diesem Host schreibt. Siehe dazu „Konfiguration der Pipeline für die Interaktion mit dem syslog-Dämonen“ auf Seite 11-8.

Sicherheitsfunktionen

Die Sicherheit ist einer der Hauptfaktoren bei der Arbeit mit der Pipeline. Die vielen für diesen Zweck zur Verfügung stehenden Sicherheitsfunktionen werden in Kapitel 9, „Einrichten der Pipeline-Sicherheit“ näher beschrieben.

SNMP-Management

Die Pipeline unterstützt in TCP/IP-Netzwerken SNMP. SNMP-Management-Stationen, die die Ascend-Enterprise-MIB verwenden, können die Pipeline abfragen, einige der Parameterwerte ändern, Alarme ertönen lassen, wenn bestimmte Zustände in der Pipeline auftreten, usw. Dazu muß auf einem Host im lokalen IP-Netzwerk ein SNMP-Manager laufen, und die Pipeline muß in der Lage sein, diesen Host entweder über eine statische Route oder über RIP zu finden.

Darüber hinaus verfügt SNMP auch über eigene Kennwort-Sicherheitsmaßnahmen, mit deren Hilfe die Pipeline vor dem Umkonfigurieren durch eine SNMP-Station geschützt werden kann.

„Remote Management“ über Telnet

Die Pipeline läßt sich durch den Aufbau einer Telnet-Sitzung von einer beliebigen entfernten Telnet-Workstation aus konfigurieren und verwalten. Die entsprechenden Konfigurationsmenüs können mit Hilfe eines Telnet-VT100-Fensters eingesehen werden.

Diese Funktion können Sie nutzen, um die Pipeline von einem lokalen oder entfernten Computer aus zu konfigurieren oder aber um entfernte Ascend-Einheiten, wie z. B. Pipelines, von einem entfernten Standort aus zu verwalten. Mit Hilfe einer solchen Telnet-Sitzung können Sie sämtliche Konfigurations-, Diagnose-, Verwaltungs- und anderen Funktionen ausführen, die auch von einem Computer aus möglich wären, der an den „Terminal“-Anschluß der Pipeline angeschlossen ist.

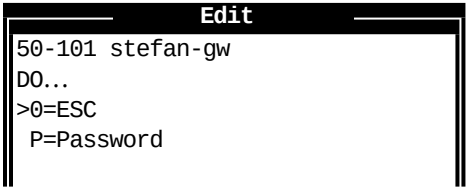
Siehe dazu „Die Terminal-Server-Befehlszeile“ auf Seite 11-31.

Aktivieren der Administrationsprivilegien

In diesem Abschnitt wird davon ausgegangen, daß Sie die Pipeline entsprechend den im Kapitel 9, „Einrichten der Pipeline-Sicherheit“, gegebenen Empfehlungen vor unbefugten Zugriff gesichert haben.

Wenn Sie den Empfehlungen gefolgt sind, können Sie nur dann administrative Operationen ausführen, wenn Sie zuvor das entsprechende Kennwort eingegeben haben. Das Kennwort wird wie folgt festgelegt:

1 Drücken Sie Strg-D, um das DO-Menü aufzurufen.

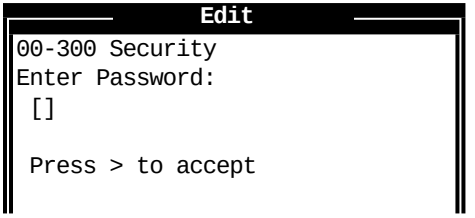


2 Drücken Sie die Taste P (bzw. wählen Sie die Option „P=Password“), um den Befehl „Password“ aufzurufen.

Es erscheint ein Menü mit Sicherheitsprofilen.

3 Wählen Sie die Option „Full Access“.

Die Pipeline fordert Sie auf, das Kennwort für das Profil „Full Access“ einzugeben.



4 Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.

Wenn Sie das richtige Kennwort eingegeben haben, erscheint eine Meldung, der zufolge das Kennwort akzeptiert wurde und die Pipeline nun mit der neuen Sicherheitsebene arbeitet. War das von Ihnen eingegebene Kennwort falsch, werden Sie erneut aufgefordert, das richtige Kennwort einzugeben.

Konfigurieren der Administrationsoptionen

In diesem Abschnitt werden die folgenden Operationen zur Systemadministration beschrieben:

- Festlegen eines Systemnamens
- Festlegen der administrativen Informationen im Systemprofil
- Festlegen des Telnet-Kennworts
- Konfiguration der Pipeline für die Interaktion mit einem Syslog-Dämonen

Tabelle 11-1 zeigt die damit in Zusammenhang stehenden Parameter.

Tabelle 11-1: Informationen zum Systemmanagement

Ort	Parameter mit Beispielwerten
System > Sys Config (Systemprofil)	Name=LAB10GW Location=LAB10 Contact=MIS Term Rate=9600 Console=Standard Remote Mgmt=No
Ethernet > Mod Config (Ethernet-Profil)	Telnet PW=*SECURE*
Ethernet > Mod Config > Log...	Syslog=Yes Log Host=10.23.45.111 Log Facility=Local5

Nähere Informationen zu den einzelnen Parametern finden Sie im *Referenzhandbuch.*

Festlegen des Systemnamens

Der Systemname der Pipeline wird beim Aushandeln von „gebridgten“ PPP-Verbindungen verwendet. Er wird wie folgt festgelegt:

1 Öffnen Sie das Systemprofil.

2 Geben Sie einen maximal 16 Zeichen langen Systemnamen an.
Beispiel:
`Name=LAB10GW`

3 Schließen Sie das Systemprofil.

Festlegen der Managementinformationen

Mit den folgenden Schritten konfigurieren Sie die Managementinformationen im Systemprofil:

1 Öffnen Sie das Systemprofil.

2 Geben Sie die physikalische Position der Pipeline an.

Beispiel:

```
Location=LAB10
```

Es können bis zu 80 Zeichen eingegeben werden. Dieses Feld kann von SNMP-Managern gelesen werden, aber sein Wert hat keinen Einfluß auf den Betrieb der Pipeline.

3 Geben Sie an, an wen sich der Benutzer im Falle von Fehlern und Problemen wenden soll.

Beispiel:

```
Contact=MIS
```

Es können bis zu 80 Zeichen eingegeben werden. Dieses Feld kann von SNMP-Managern gelesen werden, aber sein Wert hat keinen Einfluß auf den Betrieb der Pipeline.

4 Geben Sie die Datenübertragungsgeschwindigkeit des „Terminal“-Anschlusses der Pipeline an.

Beispiel:

```
Term Rate=9600
```

Der Standardwert „9600“ kann verwendet werden, wenn Sie auf die VT100-Schnittstelle von einem PC aus zugreifen, der mit dem „Terminal“-Anschluß der Pipeline verbunden ist. Soll eine Ascend-Einheit von einem anderen Standort aus verwaltet werden („Remote Management“), empfiehlt es sich, am lokalen Terminal eine höhere Datenübertragungsgeschwindigkeit einzustellen, um eine höhere Arbeitsgeschwindigkeit zu erreichen.

Hinweis: Beachten Sie, daß der Wert des Parameters „Term Rate“ mit der für den COM-Anschluß des Computers festgelegten Geschwindigkeit übereinstimmen muß.

5 Geben Sie an, was für eine Konsolenschnittstelle beim Einschalten angezeigt werden soll.

Beispiel:

```
Console=Standard
```

Dies ist zur Zeit der einzige von der Pipeline unterstützte Wert.

6 Geben Sie an, ob das entfernte Gerät die Pipeline (über das WAN) betreiben können soll („Remote Management“).

Beispiel:

```
Remote Mgmt=No
```

„Remote Management“ ist nur bei MPP-Rufen verfügbar.

7 Schließen Sie das Systemprofil.

Festlegen des Telnet-Kennworts

Um festzulegen, daß alle ankommenden Telnet-Verbindungen ein Telnet-Kennwort angeben müssen (auch für administrative Aufgaben), ist wie folgt vorzugehen:

1 Öffnen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

2 Geben Sie ein maximal 20 Zeichen langes Telnet-Kennwort an.

Beispiel:

```
Telnet PW=*SECURE*
```

3 Schließen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

Konfiguration der Pipeline für die Interaktion mit dem syslog-Dämonen

Wenn ein permanentes Protokoll der Systemereignisse der Pipeline erstellt und CDR-Berichte (Call Detail Reporting) an einen Host gesendet werden sollen, der diese aufzeichnet und verarbeitet, muß die Pipeline so konfiguriert werden, daß sie Ereignisse an einen Syslog-Host im lokalen Netzwerk meldet. Syslog-Berichte werden nur über die Ethernet-Schnittstelle gesendet.

Wenn die Pipeline Meldungen an einen Syslog-Dämonen senden soll, ist wie folgt vorzugehen:

1 Öffnen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

1. Öffnen Sie das Untermenü „Log“.
2. Aktivieren Sie den Parameter „Syslog“.
   `Syslog=Yes`
3. Geben Sie die IP-Adresse des Hosts an, auf dem der Syslog-Dämon läuft.
   Beispiel:
   `Log Host=10.1.3.7`
   Der Host, auf dem der Syslog-Dämon läuft, ist in den meisten Fällen ein UNIX-Host; es kann aber auch ein Windows-System verwendet werden. Befindet sich der Protokoll-Host nicht im selben Subnetz wie die Pipeline, muß die Pipeline entweder über eine RIP- oder über eine statische Route zu diesem Host verfügen.

   Hinweis: Der Syslog-Host darf sich nicht an einem Standort befinden, der nur über eine Wählverbindung zu erreichen ist, da die Pipeline den Host bei jeder protokollierten Aktion, u. a. auch nach jedem Aufhängen, anwählen würde.
4. Legen Sie einen Wert für den Parameter „Log Facility“ fest.
   Beispiel:
   `Log Facility=Local0`
   Dieser Parameter wird dazu verwendet, Meldungen von der Pipeline mit einem Flag zu versehen. Nach der Festlegung eines Wertes für „Log Facility“ müssen Sie den Syslog-Dämon so konfigurieren, daß er alle Meldungen, die die in „Log Facility“ angegebene Nummer enthalten, in eine bestimmte Protokolldatei (die Pipeline-Protokolldatei) schreibt.
5. Schließen Sie das Ethernet-Profil („Ethernet-->Mod Config“).

Zur Konfiguration des Syslog-Dämons ist die Datei „/etc/syslog.conf“ auf dem Syslog-Host zu modifizieren. Diese Datei gibt an, welche Aktion der Dämon ausführen soll, wenn er Meldungen von einem bestimmten, durch die „Log Facility“-Nummer gekennzeichneten Gerät (Pipeline) erhält. Wenn Sie z. B. dem Parameter „Log Facility“ den Wert „Local5“ in der Pipeline zuweisen, und die Meldungen in der Datei „/var/log/Pipeline“ gespeichert werden sollen, ist die Datei „/etc/syslog.conf“ und die folgende Zeile zu erweitern:

```
local5.info<tab>/var/log/Pipeline
```

Hinweis: Der Syslog-Dämon muß die Datei „/etc/syslog.conf“ erneut lesen, nachdem sie geändert wurde.

Die Pipeline-Statusfenster

In der Konfigurations-Schnittstelle der Pipeline werden auf der rechten Seite des Bildschirms acht Statusfenster angezeigt (Abbildung 11-1). Diese Statusfenster bieten eine Menge an Informationen darüber, was gerade in der Pipeline abläuft. Die hier angezeigten Informationen können nicht von Ihnen modifiziert werden.

Dieser Abschnitt gibt Ihnen einen Überblick über die in den acht Fenstern angezeigten Informationen. Eine vollständige Beschreibung der Angaben in den Statusfenstern finden Sie im *Referenzhandbuch*.

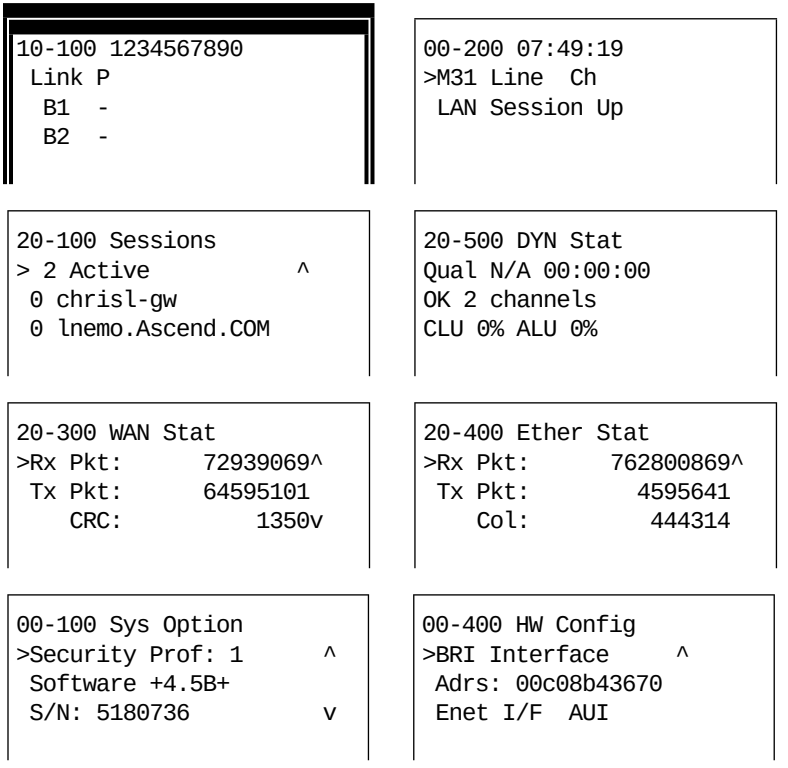


Abbildung 11-1: Statusfenster

Bewegen innerhalb der Statusfenster

Um sich innerhalb eines Statusfensters auf und ab bewegen zu können oder einen kontextspezifischen DO-Befehl auszuführen, müssen Sie das entsprechende Statusfenster aktivieren. Drücken Sie dazu so lange die Tabulatortaste, bis das gewünschte Fenster mit einer dicken Umrandung markiert ist. Mit der Tabulatortaste können Sie die einzelnen Fenster nacheinander von links nach rechts und von oben nach unten aktivieren. Wenn Sie am letzten Fenster rechts unten angelangt sind, kehren Sie mit dem nächsten Drücken der Tabulatortaste zum „Edit“-Fenster (dem Menü) zurück.

Einige der Statusfenster enthalten mehr Informationen als in dem kleinen Fenster angezeigt werden kann. Wenn in der rechten unteren Ecke eines Fensters eine kleines v zu sehen ist, heißt dies, das noch weitere Informationen vorhanden sind. Um sich diese zusätzlichen Informationen in einem Fenster anzeigen zu lassen, aktivieren Sie dieses Fenster mit Hilfe der Tabulatortaste.

„Line Status“

Das Menü „Line Status“ zeigt den dynamischen Status der einzelnen WAN-Leitungen, den Zustand der jeweiligen elektrischen Verbindung zum Carrier und den Status der einzelnen Kanäle der Leitung an.

Zeile 1

Die erste Zeile des Menüs „Line Status“ enthält die Menünummer der verbundenen Leitungen.

Zeile 2

In der zweiten Zeile des Menüs „Line Status“ wird der Gesamtstatus der Leitung angezeigt. Dies geschieht mit Hilfe von einbuchstabigen Abkürzungen, deren Bedeutung in Tabelle 11-2 erklärt wird.

Tabelle 11-2: Abkürzungen zur Anzeige des Leitungsstatus

Abkürzung	Beschreibung
P	Die Leitung befindet sich in einem aktiven Punkt-zu-Punkt-Zustand, und es besteht eine physikalische Verbindung.
D	Die Leitung befindet sich in einem aktiven Multipoint-Zustand, initialisiert im Dual-Terminal-Modus, und es besteht eine physikalische Verbindung.
M	Die Leitung befindet sich in einem aktiven Multipoint-Zustand, initialisiert im Single-Terminal-Modus, und es besteht eine physikalische Verbindung.
.	Die Leitung ist gegenwärtig nicht aktiv, es besteht jedoch eine physikalische Verbindung.
X	Es besteht keine physikalische Verbindung, so daß keine Daten weitergeleitet werden können. In einigen Ländern kann das Zeichen X auch dann erscheinen, wenn eine physikalische Verbindung besteht.
-	Die Leitung ist deaktiviert. Der Parameter „Chan Usage“ im „Configure“-Profil ist so eingestellt, daß einer der B-Kanäle deaktiviert ist.

Zeile 3 und Zeile 4

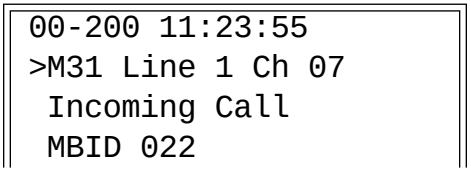
Anhand der dritten und vierten Zeile läßt sich der Status der Kanäle B1 und B2 erkennen. Der jeweilige Status wird durch ein einzelnes Zeichen angezeigt. Die Bedeutung der verwendeten Zeichen entnehmen Sie bitte der Tabelle 11-3.

Tabelle 11-3: Zeichen zur Anzeige des Leitungsstatus

Zeichen	Beschreibung
.	Der Kanal ist nicht verfügbar, da die Leitung nicht aktiv ist, keine physikalische Verbindung besteht, nicht existiert oder da der Parameter „Chan Usage“ im „Configure“-Profil so eingestellt wurde, daß einer der B-Kanäle deaktiviert ist.
*	Der Kanal ist in einem laufenden Ruf verbunden.
-	Der Kanal ruht gegenwärtig (ist aber in Betrieb).
d	Die Pipeline wählt gerade über diesen Kanal für einen abgehenden Ruf.
r	Über diesen Kanal geht gerade ein Ruf ein.
n	Der Kanal ist im „Configure“-Profil als „Leased“ (Nailed - Standleitung) gekennzeichnet.

„System Events“

Im Fenster „System Events“ werden die 32 zuletzt von der Pipeline aufgezeichneten Systemereignisse angezeigt.



Die Meldungsprotokolle werden dynamisch aktualisiert. Um sich den vorangehenden Eintrag anschauen zu können, müssen Sie die Nach-oben-Pfeiltaste drücken. Soll der folgende Eintrag angezeigt werden, ist die Nach-unten-Pfeiltaste zu drücken. Wenn Sie mit dem Palmtop-Controller arbeiten und alle Meldungen aus dem Meldungsprotokoll löschen wollen, geben Sie den Befehl SHFT-> (Löschen) ein. Verwenden Sie statt dessen den „Control Monitor“, können Sie die Meldungen im Protokoll durch Drücken der Taste „Entf“ löschen.

Das Meldungsprotokoll enthält die im folgenden beschriebenen Informationen:

Zeile 1

Die erste Zeile des Menüs zeigt die Statusmenünummer und die Uhrzeit an, zu der das Ereignis eingetreten ist.

Zeile 2

In der zweiten Zeile wird die Protokolleintragsnummer (M00-M31) sowie gegebenenfalls die Leitung und der Kanal angezeigt, auf dem das Ereignis eingetreten ist.

Die Numerierung der Leitungen beginnt mit den Basis-System-ISDN-Leitungen (Leitungen 1 und 2). Eine DDS 56-Leitung erscheint als Leitung 3.

Zeile 3

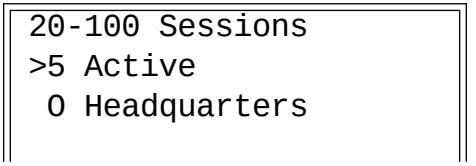
Die dritte Zeile enthält den Meldungstext. Die Meldung kann entweder reine Informationen oder eine Warnung enthalten.

Zeile 4

Die vierte Zeile enthält einen Meldungsparameter.

„Sessions“

Das Statusmenü „Sessions“ gibt die Anzahl der aktiven Bridging/Routing-Verbindungen an. Eine Online-Verbindung, deren Konfiguration im Verbindungsprofil festgelegt ist, stellt eine einzelne aktive Sitzung dar. Eine Sitzung kann PPP-Einkapselung verwenden. Die Pipeline behandelt jede Multichannel-MP+- bzw. MP-Verbindung als eine eigene Sitzung.



Die einzelnen Menüzeilen werden in den folgenden Absätzen näher beschrieben.

Zeile 1

In der ersten Zeile erscheinen die Menünummer und der Name des Menüs.

Zeile 2

Die zweite Zeile gibt die Anzahl der aktiven Sitzungen an.

Zeile 3 und folgende Zeilen

Der dritten Zeile und den folgenden Zeilen läßt sich der Status der einzelnen aktiven Sitzungen sowie der Name, die Adresse bzw. die CLID des entfernten Endes entnehmen. Die Angaben erfolgen im Format *y zzzzz*, wobei *y* ein Zeichen zur Anzeige des Sitzungsstatus ist und *zzzzz* für den Namen, die Adresse bzw. die CLID des entfernten Geräts steht.

In der Tabelle 11-4 finden Sie eine Aufstellung der möglichen Zeichen zur Anzeige des Sitzungsstatus.

Tabelle 11-4: Zeichen zur Anzeige des Sitzungsstatus

Zeichen	Beschreibung
Kein Zeichen	Es existiert kein Ruf, und es werden keine anderen Pipeline-Operationen ausgeführt.
R	„R“ steht für „Ringing“; ein Ruf geht ein und wartet auf Antwort.
A	„A“ steht für „Answering“; die Pipeline beantwortet einen ankommenden Ruf.
C	„C“ steht für „Calling“; die Pipeline wählt einen abgehenden Ruf.
O	„O“ steht für „Online“; ein Ruf liegt an.
H	„H“ steht für „Hanging up“; die Pipeline beendet den Ruf.

„Dyn Stat“

Im Menü „Dyn Stat“ wird der Name, die Qualität, die Bandbreite und die Bandbreitennutzung der jeweiligen Verbindung angezeigt.

```
20-500 Dyn Stat
Qual Good 00:02:03
56K     1 channels
CLU  12%  ALU  23%
```

Mit Hilfe der Nach-unten-Pfeiltaste können Sie sich andere Verbindungen anzeigen lassen. Es können gleichzeitig mehrere Verbindungen online sein.

Zeile 1

In der ersten Zeile des Menüs „Dyn Stat“ wird die jeweilige Menünummer und der Name des aktuellen Verbindungsprofils angezeigt. Wenn gegenwärtig keine Verbindung aktiv ist, erscheint statt dessen der Menüname.

Zeile 2

In der zweiten Zeile wird die Qualität der Verbindung und die Zeit angezeigt, die die Verbindung bereits aktiv ist. Wenn eine Verbindung mehr als 96 Stunden online ist, wird die Dauer in Tagen angezeigt. Die möglichen Werte für die Verbindungsqualität sind in Tabelle 11-5 aufgeführt.

Tabelle 11-5: Mögliche Werte für die Verbindungsqualität

Wert	Beschreibung
Good	Die aktuelle CRC-Fehlerrate liegt unter 1 %.
Fair	Die aktuelle CRC-Fehlerrate liegt zwischen 1 % und 5 %.
Marg	Die aktuelle CRC-Fehlerrate liegt zwischen 5 % und 10 %.
Poor	Die aktuelle CRC-Fehlerrate liegt über 10 %.
N/A	Die Verbindung ist nicht online.

Zeile 3

In der dritten Zeile des Menüs „Dyn Stat“ wird die aktuelle Übertragungsgeschwindigkeit in KBit/s sowie die Anzahl der Kanäle angegeben, für die diese Geschwindigkeit gilt.

Zeile 4

In der letzten Zeile werden die folgenden Werte angezeigt:

- „CLU“
  CLU (Current Line Utilization) gibt die aktuelle Leitungsnutzung an. Dieser Wert entspricht dem prozentualen Anteil der gegenwärtig von der Verbindung genutzten Bandbreite dividiert durch den Gesamtbetrag der verfügbaren Bandbreite.
- „ALU“
  ALU (Average Line Utilization) gibt die mittlere Leitungsnutzung an. Dieser Wert entspricht dem durchschnittlichen Betrag der von der Verbindung genutzten verfügbaren Bandbreite während des gegenwärtigen Zeitraums gemäß den Werten für die Parameter „Sec History“ und „Dyn Alg“.

„WAN Stat“

Im Menü „WAN Stat“ wird für jede aktive WAN-Verbindung die aktuelle Zahl der empfangenen Pakete, der gesendeten Pakete und der fehlerhaften Pakete angezeigt. Außerdem wird die Gesamtzahl aller über das WAN empfangenen und gesendeten Datenpakete angegeben.

```
20-300 WAN Stat
>Rx Pkt:  387112
 Tx Pkt:   22092
    CRC:  0
```

Die einzelnen Menüzeilen werden in den folgenden Absätzen näher beschrieben.

Zeile 1

In der ersten Zeile wird die Menünummer und der Name des Menüs angezeigt. Durch Drücken der Nach-unten-Pfeiltaste erhalten Sie für jede Verbindung statistische Angaben. In der ersten Zeile dieser Statistik erscheint der Name, die IP-Adresse oder die MAC-Adresse des entfernten Geräts. Die Werte werden alle 30 Sekunden aktualisiert. Die Aktualisierung der Gesamtzahl der gesendeten und empfangenen Pakete erfolgt jeweils am Ende der aktiven Verbindung.

Zeile 2

Die zweite Zeile zeigt die Anzahl der empfangenen Pakete an.

Zeile 3

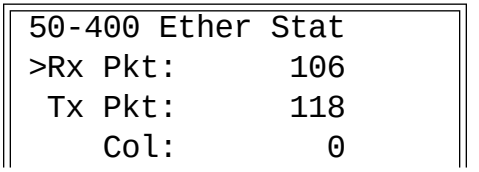
In der dritten Zeile wird die Anzahl der gesendeten Pakete angezeigt.

Zeile 4

Die vierte Zeile gibt die Anzahl der fehlerhaften Pakete an. Bei PPP- und MP+-Verbindungen erfolgt eine CRC-Überprüfung. Ein fehlerhaftes CRC-Paket enthält mindestens einen Datenfehler.

„Ether Stat“

Das Menü „Ether Stat“ gibt die Anzahl der empfangenen und gesendeten Ethernet-Pakete sowie die Anzahl der Kollisionen an der Ethernet-Schnittstelle an.



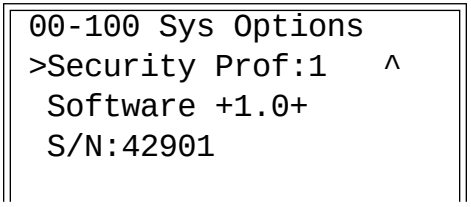
Die einzelnen Menüfelder werden in Tabelle 11-6 beschrieben.

Tabelle 11-6: Felder im Menü „Ether Stat“

Feld	Beschreibung
Rx Pkt	Zeigt die Anzahl der von der Ethernet-Schnittstelle aus empfangenen Ethernet-Pakete an.
Col	Zeigt die Anzahl der Kollisionen an, die an der Ethernet-Schnittstelle zu verzeichnen waren.
Tx Pkt	Zeigt die Anzahl der über die Ethernet-Schnittstelle gesendeten Ethernet-Pakete an.

Sys Options

Das Menü „Sys Options“ enthält Angaben zu Ihrer Pipeline und zeigt an, welche Leistungsmerkmale zur Verfügung stehen. Die Angaben im Menü können nicht geändert werden.



„Sys Options“ kann die in Tabelle 11-7 aufgeführten Angaben enthalten.

Tabelle 11-7: Angaben im Menü „Sys Options“

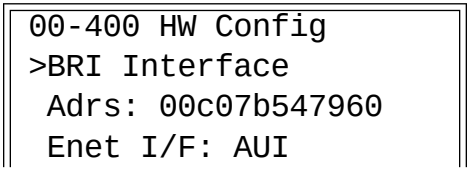
Option	Beschreibung
Security Prof: 1, Security Prof: 2...	Zeigt an, welches der neun Sicherheitsprofile die Benutzerschnittstelle steuert.
Software	Zeigt die Versions- und Revisionsnummer des System-ROM an.
S/N	Zeigt die Seriennummer der Pipeline an. Diese finden Sie auch auf dem Modell- und Seriennummernetikett auf der Unterseite der Pipeline.
Access Router	
Switched Installed oder Switched Not Inst	Zeigt an, ob die Pipeline Anrufe über gwählte Schaltungen anmelden kann.
FR Rel Installed	Zeigt an, ob die Frame-Relay-Option installiert ist.

Tabelle 11-7: Angaben im Menü „Sys Options“

Option	Beschreibung
Dyn Bnd Installed oder Dyn Bnd Not Inst	Zeigt an, ob die dynamische Bandbreitenzuweisung (DBA) verfügbar ist.
ISDN Sig Installed	Zeigt an, ob ISDN-Zeichengabe verfügbar ist.

„HW Config“

Dem Menü „HW Config“ können Sie Informationen zu der in der Pipeline installierten Hardware entnehmen.



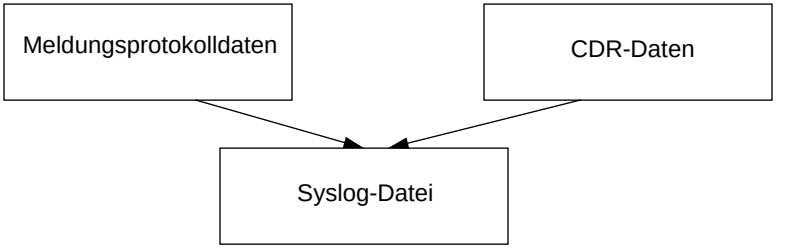
Die einzelnen Menüfelder werden in Tabelle 11-6 beschrieben.

Tabelle 11-8: Felder im Menü „Ether Stat“

Feld	Beschreibung
BRI Interface	Art der verwendeten Schnittstelle
Adr	MAC-Adresse der Pipeline
Enet I/F	Ethernet-Schnittstelle, die in der Pipeline zum Einsatz kommt (entweder UTP oder AUI).

„Syslog“

„Syslog“ ist keine Pipeline-Statusanzeige, sondern ein IP-Protokoll, das Meldungen über den Systemstatus an den Host-Computer (den „Syslog-Host“) sendet. Dieser Host wird über den Parameter „Log Host“ im Ethernet-Profil festgelegt. Der Syslog-Host speichert die Systemstatusmeldungen in einer Syslog-Datei. Für diese Meldungen gibt es zwei Quellen: die Meldungsprotokollanzeige und die CDR-Anzeige.



Hinweis: Einzelheiten zum Syslog-Dämonen finden Sie in Ihrem UNIX-Handbuch auf den Seiten über „logger(1)“, „syslog(3)“, „syslog.conf(5)“ und „syslogd(8)“. Für die Syslog-Funktion ist der UDP-Port 514 erforderlich.

Ausführen von Systemadministrations-Operationen

In diesem Abschnitt werden die folgenden Systemadministrations-Operationen beschrieben:

- manuelles Wählen und Beenden von Rufen mit Hilfe der DO-Befehle
- Wiederherstellen und Speichern einer Konfiguration
- Zurücksetzen der Pipeline
- Aufrufen der Terminal-Server-Schnittstelle

Tabelle 11-9 zeigt die im Zusammenhang mit der Systemadministration relevanten Befehle.

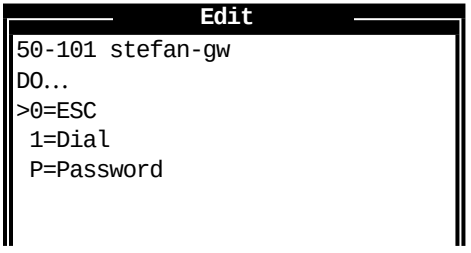
Tabelle 11-9: Befehle für die Systemadministration

Ort	Befehle
System > Sys Diag	Restore Cfg Save Cfg Sys Reset Term Serv

Nähere Informationen zu den einzelnen Befehlen finden Sie im *Referenzhandbuch.*

Verwenden der DO-Befehle

Das DO-Menü ist eine kontextsensitive Liste von Befehlen, die erscheint, wenn Sie Strg-D drücken. Die Befehle im DO-Menü hängen vom jeweiligen Kontext ab, in dem sie aufgerufen werden. Wenn Sie z. B. Strg-D in einem Verbindungsprofil drücken, sieht das DO-Menü wie folgt aus:



Um einen DO-Befehl einzugeben, müssen Sie in der VT100-Schnittstelle die Tastenkombination Strg-D drücken und loslassen und dann die nächste Taste drücken und wieder loslassen. Um z. B. den Befehl „DO 1 (Dial)“ zu wählen, ist also nach Strg-D die Taste 1 zu drücken.

Im VT-100-Monitor erfüllt die Funktionstaste PF1 die gleiche Aufgabe wie die DO-Taste oder Strg-D.

In der folgenden Liste sind alle DO-Befehle und ihre Bedeutung aufgeführt:

- 0=ESC – abbrechen und DO-Menü verlassen
- 1=Dial – ausgewähltes oder aktuelles Profil wählen
- 2=Hang Up – aufhängen (laufenden Ruf beenden)
- 3=Answer – ankommenden Ruf beantworten
- 4=Extend BW – Bandbreite erhöhen
- 5=Contract BW – Bandbreite reduzieren
- 8=Beg/End Rem Mgm – „Remote Management“ beginnen/beenden
- C=Close TELNET – aktuelle Telnet-Sitzung schließen
- R=Resynchronize – laufenden Ruf neu synchronisieren
- L=Load – Parameterwerte in aktuelles Profil laden
- P=Password – beim Pipeline-Sicherheitsprofil an- bzw. abmelden
- S=Save – Parameterwerte im angegebenen Profil speichern

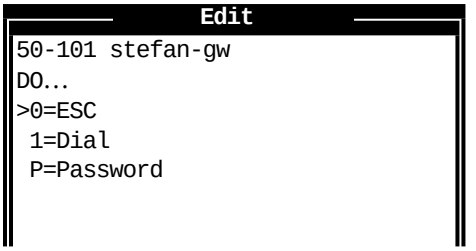
Nähere Informationen zu diesen Befehlen finden Sie im *Referenzhandbuch*.

Um einen Ruf manuell wählen zu können, muß das Verbindungsprofil für diesen Ruf offen oder in der Liste der Profile markiert sein. Soll ein Ruf beendet werden, können Sie entweder das Verbindungsprofil für die aktive Verbindung öffnen oder mit Hilfe der Tabulatortaste das Statusfenster aktivieren, in dem diese Verbindung angezeigt wird (siehe dazu „Die Pipeline-Statusfenster“ auf Seite 11-10).

Zum manuellen Wählen eines Rufes ist wie folgt vorzugehen:

1 Wählen oder öffnen Sie das „Connections“-Profil für das Ziel, das gerufen werden soll.

2 Drücken Sie Strg-D, um das DO-Menü aufzurufen.



3 Drücken Sie die Taste 1 (oder wählen Sie „1=Dial“), um den Befehl „Dial“ aufzurufen.

4 Beobachten Sie die Informationen im Statusfenster „Sessions“. Bei ordnungsgemäßem Verlauf erscheint dort die gerufene Nummer sowie eine Meldung, daß die Netzwerksitzung hergestellt wurde.

Wenn Sie die Option „1=Dial“ nicht sehen können, kann dies auf eine der folgenden Ursachen zurückzuführen sein:

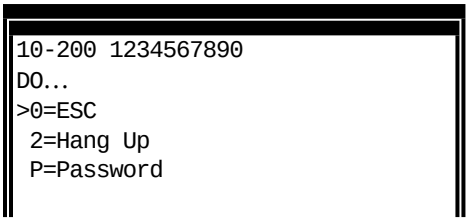
- Sie befinden sich nicht im richtigen Profil.
- Sie haben nicht die richtige Sicherheitsebene aktiviert.
- Im Profil ist keine Rufnummer angegeben.
- Im Profil ist keine IP-Adresse angegeben (wenn IP-Routing aktiviert ist).

Mit den folgenden Schritten können Sie einen Ruf manuell beenden:

1 Öffnen Sie das „Connections“-Profil, oder aktivieren Sie mit Hilfe der Tabulatortaste das Statusfenster, in dem die Informationen über die aktive Sitzung, die gelöscht werden soll, angezeigt werden.

2 Drücken Sie Strg-D, um das DO-Menü zu öffnen.

Wenn Sie das DO-Menü für eine aktive Sitzung öffnen, sieht es ungefähr so aus:



3 Drücken Sie die Taste 2 (oder wählen Sie „2=Hang Up“), um den Befehl „Hang Up“ aufzurufen.

Das Statusfenster zeigt an, daß der Ruf beendet wurde.

Sichern der Pipeline-Konfiguration

Um die Pipeline-Konfiguration sichern zu können, müssen Sie über administrative Privilegien verfügen, die auch den Vor-Ort-Service mit einschließen (wie z. B. das Profil „Full Access“).

Hinweis: Beim Sichern der Pipeline-Konfiguration werden die Konfigurationsdaten in eine Textdatei auf der Festplatte des Host-Computers geschrieben, der mit dem „Terminal“-Anschluß der Pipeline verbunden ist. *Kennwörter werden nicht mit gesichert!* Wenn Sie eine Konfiguration anhand einer gesicherten Datei wiederherstellen, werden die Parameter „Send PW“, „Recv PW“ sowie die Kennwörter für die Sicherheitsprofile und die im Ethernet-Profil (Menü „Mod Config“) festgelegten Kennwörter alle auf das „Null-Kennwort“ gesetzt (für den Zugang reicht dann das Drücken der Eingabetaste). Wir empfehlen daher dringend, sich diese Kennwörter zu notieren und sicher aufzubewahren, falls sie wiederhergestellt werden müssen.

Bevor Sie beginnen, sollten Sie sicherstellen, daß Ihre Terminal-Emulation das Speichern der am seriellen Anschluß empfangenen ASCII-Zeichen auf der Festplatte erlaubt. Außerdem ist zu kontrollieren, daß die Datenübertragungsgeschwindigkeit des Terminal-Emulationsprogramms auf maximal 9600 Bit/s eingestellt ist, und daß für den Parameter „Term Rate“ im Systemprofil (Menü „Sys Config“) ebenfalls der Wert „9600“ festgelegt wurde. Bei höheren Geschwindigkeiten können Fehler beim Speichern der Zeichen auftreten.

Sie können den Sicherungsvorgang jederzeit abbrechen. Drücken Sie dazu die Tastenkombination Strg-C.

Mit den folgenden Schritten können Sie die Pipeline-Konfiguration (mit Ausnahme der Kennwörter) auf der Festplatte speichern:

1 Öffnen Sie das Menü „Sys Diag“.

2 Wählen Sie den Befehl „Save Config“, und drücken Sie die Eingabetaste.
Es erscheint die folgende Meldung:

```
Ready to download - type any key to start...
```

3 Aktivieren Sie die Zeichenspeicherungsfunktion Ihres DFÜ-Programms, und geben Sie einen Dateinamen für die gespeicherten Profile an.
Wenn Sie Fragen zur Aktivierung der Zeichenspeicherungsfunktion haben, schlagen Sie in der Dokumentation zu Ihrem DFÜ-Programm nach.

4 Drücken Sie eine beliebige Taste, um das Speichern der konfigurierten Profile zu starten.
Auf dem Bildschirm erscheinen während des Speicherns auf die Festplatte die verschiedensten Konfigurationsinformationen. Nach Abschluß des Speichervorgangs erscheint eine entsprechende Meldung.

5 Deaktivieren Sie die Zeichenspeicherfunktion Ihres DFÜ-Programms.

6 Drucken Sie ein Exemplar der konfigurierten Profile aus, um gegebenenfalls später darauf zurückgreifen zu können.

Hinweis: Bei der Betrachtung der gespeicherten Pipeline-Datendatei werden Sie feststellen, daß einige der Zeilen mit *START=* und andere mit *END=* beginnen. Diese START/STOP-Zeilen und der dazwischenliegende Datenblock sind ein Profil. Wenn ein Parameter in einem Profil auf seinen Standardwert gesetzt wird, erscheint dieser nicht im Profil. Wenn also für alle Parameter in einem Profil der Standardwert festgelegt wurde, ist der entsprechende START/STOP-Block leer. Stellen Sie sicher, daß sich vor *START=* und nach *END=* keine zusätzlichen Textzeilen oder Zeichen befinden. Wenn sich dort Zeichen oder Zeilen befinden, sind diese zu löschen, da Sie zu Problemen bei der Wiederherstellung der Datei führen könnten.

Wiederherstellen der Pipeline-Konfiguration

Um die Pipeline-Konfiguration wiederherstellen zu können, müssen Sie über administrative Privilegien verfügen, die auch den Vor-Ort-Service mit einschließen (wie z. B. das Profil „Full Access“).

Vor dem Beginn der Wiederherstellungsprozedur sollten Sie sich vergewissern, daß Ihr Terminalemulationsprogramm über eine Autotype-Funktion (bzw. eine ASCII-Dateien-Upload-Funktion) verfügt. Mit Hilfe der Autotype-Funktion kann Ihr Emulationsprogramm Textdateien über den seriellen Anschluß senden. Außerdem ist sicherzustellen, daß die Datenübertragungsgeschwindigkeit des Terminalemulationsprogramms auf maximal 9600 Bit/s eingestellt ist. Der Parameter „Term Rate“ im Systemprofil (Menü „Sys Config“) muß ebenfalls auf 9600 eingestellt sein. Höhere Geschwindigkeiten können zu Übertragungsfehlern führen.

Der Befehl „Restore Cfg“ kann verwendet werden, um eine vollständige Konfiguration, die Sie zuvor mit dem Befehl „Save Cfg“ gespeichert haben, wiederherzustellen oder um spezifischere Konfigurationsinformationen, die Sie von Ascend erhalten haben (z. B. einen einzelnen, in einer speziellen Konfigurationsdatei gespeicherten Filter), hochzuladen.

Zum Laden der Konfigurationsinformationen von der Festplatte ist wie folgt vorzugehen:

1. Schließen Sie das Backup-Gerät an den „Terminal“-Anschluß der Pipeline an.

   Beim Backup-Gerät handelt es sich zumeist um den PC, mit dem Sie auf die VT100-Schnittstelle zugreifen.

2. Öffnen Sie das Menü „Sys Diag“.

3. Wählen Sie den Befehl „Restore Cfg“, und drücken Sie die Eingabetaste.

   Es erscheint die folgende Meldung:

   ```
   Waiting for upload data...
   ```

4 Senden Sie mit Hilfe der Funktion „ASCII-Datei senden“ Ihres DFÜ-Programms die Konfigurationsdatei an die Pipeline.

Sollten Sie Fragen zum Senden von ASCII-Dateien haben, finden Sie die entsprechenden Informationen in der Dokumentation zu Ihrem DFÜ-Programm. Nach Abschluß der Wiederherstellung erscheint die folgende Meldung:

```
Restore complete - type any key to return to menu
```

5 Drücken Sie eine beliebige Taste, um zum Konfigurationsmenü zurückzukehren.

Wenn Sie eine vollständige Konfiguration wiederhergestellt haben, sind die Kennwörter in Ihren Sicherheitsprofilen nicht mehr vorhanden. Sollen Sie erneut festgelegt werden, ist wie folgt vorzugehen:

1 Drücken Sie die Tastenkombination Strg-D. Es erscheint das DO-Menü. Markieren Sie die Option „Password“, und wählen Sie das Profil „Full Access“.

2 Drücken Sie die Eingabetaste („Null-Kennwort“), sobald Sie aufgefordert werden, ein Kennwort einzugeben.

Nachdem Sie Ihre Zugriffsrechte wiederhergestellt haben, indem Sie festgelegt haben, daß das „Null-Kennwort“ verwendet werden soll, empfehlen wir, sofort die Verbindungsprofile, Sicherheitsprofile und das Ethernet-Profil (Menü „Mod Config“) zu öffnen und die vorherigen Einstellungen für die Kennwörter wiederherzustellen.

Weitere Informationen dazu finden Sie in Anhang E, „Aktualisieren der Systemsoftware“.

Zurücksetzen der Pipeline

Wenn Sie die Pipeline zurücksetzen, wird die Einheit neu gestartet, und alle aktiven Verbindungen werden beendet. Alle Benutzer werden ausgeloggt, und es wird die Standard-Sicherheitsebene aktiviert. Das Zurücksetzen des Systems kann darüber hinaus dazu führen, daß der WAN-Anschluß aufgrund des vorübergehenden Verlustes von Zeichengabe- oder Framing-Informationen zeitweise außer Kraft gesetzt wird.

Mit den folgenden Schritten können Sie die Einheit zurücksetzen:

1 Öffnen Sie das Menü „Sys Diag“.

2 Markieren Sie die Option „Sys Reset“, und drücken Sie die Eingabetaste. Die Pipeline fordert Sie auf, das Zurücksetzen zu bestätigen.

```
0=ESC
1=Reset
```

3 Drücken Sie die Taste 1.

Beim Zurücksetzen werden die aktiven Verbindungen gelöscht, und es wird der Einschalt-Selbsttest (Power-On Self Test, POST) durchgeführt. Erscheint die POST-Anzeige nicht auf dem Bildschirm, aktualisieren Sie die Anzeige mit Strg-L.

Während des Tests des Speichers, der Konfiguration, der installierten Module und der Leitungen leuchtet die gelbe LED „FAULT“ an der Frontblende der Pipeline. Wenn einer der Tests nicht erfolgreich ist, bleibt die LED „FAULT“ leuchten, bzw. sie fängt an zu blinken.

Das Alarmrelais bleibt während des POST geschlossen. Es öffnet sich erst, wenn der POST erfolgreich abgeschlossen wurde. Dies wird mit der folgenden Meldung angezeigt:

```
Power-On Self Test PASSED
Press any key...
```

Drücken Sie eine beliebige Taste, um das „Main Edit Menu“ zu öffnen.

Die Terminal-Server-Befehlszeile

In diesem Abschnitt wird beschrieben, wie Sie die administrativen Befehle verwenden können, die in der Befehlszeilenschnittstelle des Terminal-Servers zur Verfügung stehen. Folgende Aufgaben werden näher erläutert:

- Aufrufen und Verlassen der Terminal-Server-Schnittstelle
- Initiieren von Selbsttest-Rufen
- Aufbauen einer „Remote Management“-Sitzung mit einem Gerät am anderen Ende einer MP+-Verbindung
- Festlegen von Parametern, z. B. zur Einstellung des Terminaltyps
- Anzeigen von Informationen, wie z. B. den ARP-Speicher, Statistiken über spezifische Protokolle oder ISDN-Ereignisse
- Verwendung von IP-Routen
- „Pingen“ von IP- bzw. IPX-Hosts
- Einloggen bei einem IP-Host über TELNET

Aufrufen und Verlassen der Terminal-Server-Schnittstelle

Zum Aufrufen der Befehlszeilenschnittstelle des Terminal-Servers müssen Sie über administrative Privilegien verfügen. Siehe dazu „Aktivieren der Administrationsprivilegien“ auf Seite 11-4.

Zum Öffnen der Befehlszeilenschnittstelle ist wie folgt vorzugehen:

1 Öffnen Sie das Menü „Sys Diag“.

2 Markieren Sie die Option „Term Serv“, und drücken Sie die Eingabetaste.

Am unteren Rand des VT100-Fensters erscheint die Befehlszeilen-Eingabeaufforderung:

```
ascend%
```

3 Zum Schließen der Befehlszeilenschnittstelle ist an der Eingabeaufforderung der Befehl „QUIT“ einzugeben.

Beispiel:

```
ascend% quit
```

Die Befehlszeilenschnittstelle wird geschlossen, und der Cursor kehrt wieder zu den VT100-Menüs zurück.

Hinweis: Zum Beenden der Sitzung können auch die Befehle „HANGUP“ und „LOCAL“ verwendet werden. Wenn ein sich einwählender Benutzer den Befehl „LOCAL“ eingibt, wird eine Telnet-Verbindung zur Pipeline aufgebaut.

Hilfe

Mit dem Befehl „?“ können Sie sich eine Liste der Terminal-Server-Befehle anzeigen lassen. Wenn Sie

```
ascend% ?
```

eingeben, erscheint die folgende Liste:

```
?           Anzeige von Hilfe-Informationen
help           "     "    "        "
quit        Schließen der Terminal-Server-Sitzung
hangup          "      "     "       "       "
test        test <Rufnummer> [<Anzahl Rahmen>] [<optionale Felder>]
local       Aufrufen des lokalen Modus
remote      remote <Station>
set         Festlegen verschiedener Einstellungen. Mit „set ?“ können
            Sie sich Hilfe-Informationen anzeigen lassen.
show        Anzeigen verschiedener Tabellen. Mit „show ?“ können Sie
            sich Hilfe-Informationen anzeigen lassen.
iproute     Verwalten von IP-Routen. Mit „iproute ?“ können Sie sich
            Hilfe-Informationen anzeigen lassen.
telnet      telnet [ -a|-b ] <Hostname> [<Port-Nummer>]
tcp         tcp <Hostname> <Port-Nummer>
ping        ping [-qv] [-c Anzahl der Pakete] [-i Verzögerung] [-s
            Paketgröße]
ipxping     ipxping <Servername>
```

Wenn Sie Hilfe zu einem bestimmten Befehl benötigen, geben Sie diesen Befehl zusammen mit einem Fragezeichen ein. Beispiel:

```
show ?
```

Initiieren von Selbsttest-Rufen

Wenn Sie einen Selbsttest durchführen lassen wollen, bei dem die Pipeline einen Ruf zu sich selbst initiiert, muß die Pipeline über zwei offene Kanäle verfügen: einen für das Initiieren und einen für das Empfangen des Rufes. Der entsprechende „TEST“-Befehl hat das folgende Format:

```
test <Rufnummer> [<Anzahl Rahmen>] [<optionale Felder>]
```

Die einzugebende Rufnummer hängt von der Ausführung Ihres Anschlusses ab:

- Wenn Ihr ISDN-Anschluß nur eine Telefonnummer zugewiesen bekommen hat, geben Sie den Wert des Parameters „My Num A“ (im „Configure“-Profil) ein.
- Wenn Ihr ISDN-Anschluß zwei Telefonnummern zugewiesen bekommen hat, geben Sie den Wert des Parameters „My Num B“ (im „Configure“-Profil) ein.

Beispiel:

```
ascend% test 555-1212
```

Mit Strg-C können Sie den Test jederzeit beenden. Während der Test läuft, zeigt die Pipeline den jeweiligen Status an. Beispiel:

```
calling...answering...testing...end
200 packets sent, 200 packets received
```

Argumente für den Befehl „TEST“

Der Befehl „TEST“ kann die folgenden Argumente haben:

- <Rufnummer>

  Die Telefonnummer des Kanals, über den der Testruf empfangen werden soll. Es können die Ziffern 0 bis 9 und die Zeichen `()[]-` eingegeben werden; Leerzeichen sind nicht erlaubt. Wenn Ihr ISDN-Anschluß über zwei Telefonnummern verfügt, muß die zweite Nummer angegeben werden. Bei ISDN-Anschlüssen mit nur einer Telefonnummer können Sie diese angeben. Während des Tests wird auf dem Kanal 1 ein Ruf initiiert, der von Kanal 2 beantwortet wird.

- [<Anzahl Rahmen>]

  (optional) Die Anzahl der Rahmen, die während des Tests gesendet werden sollen. Es kann eine Zahl von 1 bis 65535 angegeben werden. Der Standardwert ist 100.

- [data-svc=<data-svc>]

  Für „data-svc“ ist einer der möglichen Wert für den Parameter „Data Svc“ im Verbindungsprofil einzugeben. Eine Liste der gültigen Werte finden Sie im *Referenzhandbuch*. Wenn Sie keinen Wert angeben, wird als Standardwert der Wert des Parameters „Data Svc“ verwendet.

„TEST“-Fehlermeldungen

Die Pipeline erstellt eine Fehlermeldung für jeden Zustand, der dazu führt, daß der Test beendet wird, bevor die festgelegte Zahl von Paketen gesendet wurde. Folgende Fehlermeldungen können erscheinen:

`bad digits in phone number`	Die von Ihnen angegebene Telefonnummer enthielt ein nicht erlaubtes Zeichen. Erlaubt sind nur die Ziffern 0 bis 9 und die Zeichen `()[]-.`
`call failed`	Die Pipeline hat den abgehenden Ruf nicht beantwortet. Dieser Fehler kann auf eine falsche oder eine besetzte Telefonnummer zurückzuführen sein. Mit Hilfe des Befehls „SHOW ISDN“ können Sie die Ursache des Fehlers feststellen.
`call terminated <N1> packets sent <N2> packets received`	Diese Meldung zeigt die Anzahl der gesendeten (<N1>) und die der empfangenen (<N2>) Pakete an.
`can’t handshake`	Die Pipeline hat den abgehenden Ruf beantwortet, die beiden Seiten konnten sich jedoch nicht ordnungsgemäß gegenseitig erkennen. Dieser Fehler kann darauf zurückzuführen sein, daß der Ruf an das falsche Pipeline-Modul weitergeleitet oder eine falsche Telefonnummer angegeben wurde.
`frame-count must be in the range 1-65535`	Die Anzahl der angeforderten Rahmen lag über 65535.
`no phone number`	In der Befehlszeile wurde keine Telefonnummer angegeben.
`test aborted`	Der Test wurde beendet (Strg-C).
`unit busy`	Sie haben versucht, einen weiteren Selbsttest zu starten, obwohl bereits ein anderer Selbsttest lief. Es kann immer nur ein Selbsttest gleichzeitig durchgeführt werden.
`unknown items on command line`	Die Befehlszeile enthielt unbekannte Elemente. Dieser Fehler kann auftreten, wenn die angegebene Telefonnummer Leerzeichen enthält.
`unknown option <Option>`	Die Befehlszeile enthielt die durch <Option> angegebene Option, die nicht gültig ist.
`unknown value <Wert>`	Die Befehlszeile enthielt den durch <Wert> angegebenen Wert, der nicht gültig ist.
`wrong phone number`	Der Ruf wurde nicht von der Pipeline, sondern von einem anderen Gerät beantwortet; die von Ihnen angegebene Telefonnummer war also falsch.

Starten einer „Remote Management“-Sitzung

Nachdem eine MP+-Verbindung mit der entfernten Station hergestellt wurde (z. B. mit Hilfe des Befehls „DO DIAL“), können Sie eine „Remote Management“-Sitzung mit dieser Station starten, indem Sie in der Befehlszeile den Befehl „REMOTE“ eingeben. Dazu ist das folgende Format zu verwenden:

```
remote <Station>
```

Beispiel:

```
ascend% remote lab17gw
```

Während der „Remote Management“-Sitzung wird die lokale Benutzerschnittstelle durch die Benutzerschnittstelle des entfernten Geräts ersetzt, so als hätten Sie eine Telnet-Verbindung mit dem Gerät geöffnet. Die „REMOTE“-Sitzung kann mit Strg-\ jederzeit abgebrochen werden. Die Sitzung kann auch von beiden Seiten der MP+-Verbindung aus durch Aufhängen aller Kanäle der Verbindung beendet werden.

Das Argument des Befehls „REMOTE“ ist der Name der entfernten Station. Dieser muß mit dem Wert des Parameters „Station“ in einem Verbindungsprofil übereinstimmen, das das Initiieren von abgehenden MP+-Rufen unterstützt.

Hinweis: Eine „Remote Management“-Sitzung kann aufgrund der Überschreitung der im Parameter „Idle“ festgelegten Zeit beendet werden, da der von ihr erzeugte Verkehr nicht den „Idle“-Timer zurücksetzt. Daher sollte der Parameter „Idle“ in den Verbindungsprofilen auf der rufenden und der antwortenden Seite der Verbindung während einer „Remote Management“-Sitzung deaktiviert und erst kurz vor Beendigung der Sitzung wiederhergestellt werden. Für „Remote Management“ empfiehlt sich die Verwendung höherer Terminalgeschwindigkeiten.

Privilegien für das „Remote Management“

Zu Beginn einer „Remote Management“-Sitzung verfügen Sie über die im Standard-Sicherheitsprofil am entfernten Ende der Verbindung festgelegten Privilegien. Um administrative Aufgaben auf der entfernten Station durchführen zu können, muß das entsprechende entfernte Sicherheitsprofil aktiviert werden. Verwenden Sie dazu den Befehl „DO PASSWORD“.

„REMOTE“-Fehlermeldungen

Die Pipeline gibt für jeden Zustand, der dazu führt, daß die „Remote Management“-Sitzung beendet wird, bevor die festgelegte Zahl von Paketen gesendet wurde, eine Fehlermeldung aus. Folgende Fehlermeldungen können erscheinen:

`not authorized`	Ihre gegenwärtigen Sicherheitsprivilegien reichen nicht aus, um eine „Remote Management“-Sitzung zu starten. Um die erforderlichen Privilegien zu erhalten, müssen Sie sich mit dem Befehl „DO PASSWORD“ bei einem Sicherheitsprofil anmelden, bei dem der Parameter „Edit System“ den Wert „Yes“ hat.
`can’t find profile for <Station>`	Die Pipeline konnte kein lokales Verbindungsprofil finden, bei dem der Wert des Parameters „Station“ mit dem Wert von <Station> übereinstimmt.
`profile for <Station> doesn’t specify MPP`	Im lokalen Verbindungsprofil, bei dem der Wert des Parameters „Station“ mit dem Wert von <Station> übereinstimmt, wurde nicht „Encaps=MPP“ festgelegt.
`can’t establish connection for <Station>`	Die Pipeline hat ein lokales Verbindungsprofil gefunden, das die richtigen Einstellungen für die Parameter „Station“ und „Encaps“ enthält, aber die Verbindung zur entfernten Station konnte dennoch nicht hergestellt werden.
`<Station> didn’t negotiate MPP`	Die entfernte Station hat keine MP+-Verbindung ausgehandelt. Dieser Fehler tritt am häufigsten auf, wenn die entfernte Station zwar PPP, aber nicht MP+ unterstützt.
`far end doesn’t support remote management`	Die entfernte Station verwendet eine MP+-Version, die „Remote Management“ nicht unterstützt.

`management session failed`	Die „Remote Management“-Sitzung konnte aufgrund eines temporären Zustands, wie z. B. der vorzeitigen Beendigung der Verbindung, nicht erfolgreich abgeschlossen werden.
`far end rejected session`	Bei der Konfiguration der entfernten Station wurde festgelegt, daß „Remote Management“-Versuche zurückgewiesen werden sollen („Remote Mgmt=No“ im Systemprofil).

Aktivieren von Kennwortabfragen

Der „SET“-Befehl kann zur Festlegung eines Terminaltyps und zur Aktivierung der dynamischen Kennwortbereitstellung verwendet werden. Mit dem Befehl „SET ALL“ lassen sich die aktuellen Einstellungen anzeigen. Beispiel:

```
ascend% set all
term = vt100
dynamic password serving = disabled
```

Mit dem Befehl „SET PASSWORD“ wird der Terminal-Server in den Kennwortmodus versetzt, in dem ein ACE- oder SAFEWORD-Server in einem sicheren Netzwerk dynamisch Kennwortabfragen in der Terminal-Server-Schnittstelle anzeigen kann. Dieser Befehl ist nur für die Authentifizierung mittels Sicherheitskarten verfügbar. In den Kennwortmodus gelangen Sie, indem Sie den folgenden Befehl eingeben:

```
ascend% set password
```

Im Kennwortmodus wartet der Terminal-Server passiv auf Kennwortabfragen von einem entfernten ACE- oder SAFEWORD-Server. Zur Rückkehr zum normalen Terminal-Server-Betrieb und damit zur Deaktivierung des Kennwortmodus ist Strg-C zu drücken.

Hinweis: Beachten Sie, daß für jeden Kanal einer Verbindung zu einem sicheren Netzwerk ein eigenes Kennwort anzugeben ist. Daher muß der Terminal-Server bei Mehrkanalverbindungen zu einem sicheren Netzwerk so lange im Kennwortmodus bleiben, bis alle Kanäle verbunden sind. Mit Hilfe des Dienstprogramms APP Server können Sie die Benutzer in die Lage versetzen, auf Kennwortabfragen mit dem auf der persönlichen Sicherheitskarte des Benutzers angezeigten dynamischen Kennwort zu antworten. Nähere Informationen dazu finden Sie im Kapitel 9, „Einrichten der Pipeline-Sicherheit“.

Anzeigen des ARP-Speichers

Der ARP-Speicher (Address Resolution Protocol) ermöglicht die Zuweisung von IP-Adressen zu physikalischen Netzwerkadressen. Wenn Sie sich dessen Inhalt anzeigen lassen wollen, können Sie den folgenden Befehl eingeben:

```
ascend% show arp
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
IP Address    Hardware Address    Type    Interface  RefCount
10.2.3.4      00:40:c7:5a:64:6c   Static  ie0        65
100.5.6.7     00:ab:77:cf:12:47   Dynamic wan0       39
```

Die Felder haben die folgende Bedeutung:

IP Address	IP-Adresse in einer ARP-Anforderung
Hardware Address	MAC-Adresse in einer ARP-Anforderung
Type	„Dynamic“ oder „Static“ – zeigt an, wie die Adresse erhalten wurde
Interface	Schnittstelle, über die die Pipeline das ARP-Paket empfangen hat; „ie0“ steht für die Ethernet-Schnittstelle, „wanN“ steht für eine aktive WAN-Schnittstelle
Ref Count	Angabe, wie oft die Adresse verwendet wurde

Anzeigen von statistischen Angaben zur Schnittstelle

Mit dem folgenden Befehl können Sie sich den Status und die Anzahl der gesendeten und empfangenen Pakete für jede aktive WAN-Verbindung sowie Angaben zur lokalen und zur Rückschleifen-Schnittstelle anzeigen lassen:

```
ascend% show if stats
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Interface  Name      Status  Type   Speed     MTU   InPackets   Outpacket
ie0        ethernet  Up       6     10000000  1500       7385       85384
wan0                 Down     1           0  1500          0           0
wan1                 Down     1           0  1500          0           0
wan2                 Down     1           0  1500          0           0
wanidle0             Up       6     10000000  1500          0           0
lo0        loopback  Up      24     10000000  1500          0           0
```

Die Felder haben die folgende Bedeutung:

Interface	„ie0“ steht für die Ethernet-Schnittstelle, „lo0“ steht für die Rückschleifen-Schnittstelle, „wanN“ gibt die einzelnen aktiven WAN-Schnittstellen in der Reihenfolge an, in der sie aktiv wurden, und „wanidle0“ ist die inaktive Schnittstelle. Die inaktive Schnittstelle ist die Schnittstelle, zu der alle Pakete umgeleitet werden, wenn die WAN-Verbindungen unterbrochen sind.
Name	Name des Profils, das mit der Schnittstelle verbunden ist, bzw. ein Textname für die Schnittstelle
Status	Status der Schnittstelle: „Up“ bedeutet, daß die Schnittstelle betriebsbereit ist, ohne dabei unbedingt gerade mit einem aktiven Ruf beschäftigt zu sein. „Down“ bedeutet, daß die Schnittstelle nicht betriebsbereit ist.
Type	Typ der an der Schnittstelle verwendeten Anwendung gemäß RFC 1213 (MIB-2); z. B. steht „23“ für PPP und „28“ für SLIP
Speed	Datenübertragungsgeschwindigkeit in Bit/s
MTU	*Maximum Transmission Unit*: von der Schnittstelle unterstützte maximale Paketgröße

InPackets	Anzahl der von der Schnittstelle empfangenen Pakete
OutPackets	Anzahl der von der Schnittstelle gesendeten Pakete

Zur Anzeige der Pakete, die die Schnittstelle passiert haben, aufgeschlüsselt nach den einzelnen Pakettypen, können Sie den folgenden Befehl eingeben:

```
ascend% show if totals
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Name        --Octets-- --Ucast---NonUcast-Discard -Error-Unknown-Same IF-
ie0      i:   7813606   85121      22383       0      0       0        0
         o: 101529978   85306        149       0      0       0        0
wan0     i:          0       0          0       0      0       0        0
         o:          0       0          0       0      0       0        0
wan1     i:          0       0          0       0      0       0        0
         o:          0       0          0       0      0       0        0
wan2     i:          0       0          0       0      0       0        0
         o:          0       0          0       0      0       0        0
wanidle0 i:          0       0          0       0      0       0        0
         o:          0       0          0       0      0       0        0
lo0      i:          0       0          0       0      0       0        0
          o:           0         0         0          0      0       0
```

Die Felder haben die folgende Bedeutung:

Name	Name der Schnittstelle (derselbe wie oben beschrieben)
Octets	Gesamtzahl der von der Schnittstelle verarbeiteten Bytes
Ucast	Pakete mit einer Unicast-Zieladresse
NonUcast	Pakete mit einer Multicast-Adresse oder einer Broadcast-Adresse
Discard	Anzahl der Pakete, die von der Schnittstelle nicht verarbeitet werden konnten
Error	Anzahl der Pakete mit CRC-Fehlern, Header-Fehlern oder Kollisionen

Unknown	Anzahl der Pakete, die von der Pipeline über alle „gebridgten“ Schnittstellen weitergeleitet wurden, da die Zieladresse nicht bekannt war oder nicht anderweitig bezogen werden konnte
Same IF	Anzahl der „gebridgten“ Pakete, deren Zieladresse identisch mit der Ausgangsadresse war

Anzeigen der TCP/IP-Informationen

In diesem Abschnitt wird beschrieben, was Sie beim Anzeigen der Informationen über die folgenden Protokolle zu beachten haben:

- ICMP
- IP
- TCP
- UDP

ICMP-Statistiken

Wenn Sie sich die Anzahl der ICMP-Pakete (Internet Control Message Protocol) anzeigen lassen wollen, die entweder gesendet oder intakt bzw. mit Fehlern empfangen bzw. gesendet wurden, ist der folgende Befehl einzugeben:

```
ascend% show icmp
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
3857661 packets received.
20 packets received with errors.
   Input histogram: 15070
2758129 packets transmitted.
0 packets transmitted due to lack of resources.
   Output histogram: 15218
```

Die Eingangs- und Ausgangshistogramme („Input Histogram“ und „Output Histogram“) zeigen die Anzahl der empfangenen und gesendeten ICMP-Pakete in jeder der drei Kategorien an.

IP-Statistiken

Wenn Sie sich statistische Informationen zur IP-Aktivität, einschließlich der Anzahl der von der Pipeline empfangenen und gesendeten IP-Pakete, anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show ip stats
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
107408 packets received.
     0 packets received with header errors.
     0 packets received with address errors.
     0 packets forwarded.
     0 packets received with unknown protocols.
     0 inbound packets discarded.
107408 packets delivered to upper layers.
 85421 transmit requests.
     0 discarded transmit packets.
     1 outbound packets with no route.
     0 reassembly timeouts.
     0 reassemblies required.
     0 reassemblies that went OK.
     0 reassemblies that Failed.
     0 packets fragmented OK.
     0 fragmentations that failed.
     0 fragment packets created.
     0 route discards due to lack of memory.
     64 default ttl.
```

Informationen zu den IP-Adressen

Wenn Sie sich die Ausgangs- und Ziel-IP-Adressen für die aktiven IP-Routing-Verbindungen anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show ip address
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Interface   IP Address    Dest IP Address   Netmask          MTU  Status
ie0           10.2.3.4    N/A               255.255.255.224  1500    Up
wan0          0.0.0.0     N/A               0.0.0.0          1500    Down
wan1          0.0.0.0     N/A               0.0.0.0          1500    Down
wan2          0.0.0.0     N/A               0.0.0.0          1500    Down
wanidle0      10.5.7.9    N/A               255.255.255.224  1500    Up
lo0           127.0.0.1   N/A               255.255.255.255  1500    Up
```

Die Felder haben die folgende Bedeutung:

Interface	„ie0“ steht für die Ethernet-Schnittstelle, „lo0“ für die Rückschleifen-Schnittstelle, „wanN“ gibt die einzelnen aktiven WAN-Schnittstellen in der Reihenfolge an, in der sie aktiv wurden, und „wanidle0“ ist die inaktive Schnittstelle (die Schnittstelle, zu der alle Pakete umgeleitet werden, wenn die WAN-Verbindungen der jeweiligen Routen unterbrochen sind).
IP Address	IP-Adresse der Schnittstelle
Dest IP Address	IP-Adresse des entfernten Routers (nur für Schnittstellen mit aktiver Verbindung verfügbar, bei der IP-Routing aktiviert ist)
Netmask	für die Schnittstelle verwendete Netzmaske
MTU	*Maximum Transmission Unit*: von der Schnittstelle unterstützte maximale Paketgröße
Status	Status der Schnittstelle: „Up“ bedeutet, daß die Schnittstelle betriebsbereit ist, ohne dabei unbedingt gerade mit einem aktiven Ruf beschäftigt zu sein. „Down“ bedeutet, daß die Schnittstelle nicht betriebsbereit ist.

Informationen zum IP-Routing

Wenn Sie sich die gesamte IP-Routing-Tabelle der Pipeline anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show ip routes
```

Soll nur die Route zu einer bestimmten Adresse angezeigt werden, können Sie diesen Befehl im folgenden Format eingeben:

```
show ip routes <Hostname>
```

<Hostname> ist ein Hostname oder eine IP-Adresse.

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Destination       Gateway       IF      Flg Pref  Met   Use
Age
0.0.0.0/0        10.0.0.100     wan0     SG   1    1     0
20887
10.207.76.0/24    10.207.76.1   wanidle0 SG   100  7     0
20887
10.207.76.1/32    10.207.76.1   wanidle0 S    100  7     2
20887
10.207.77.0/24    10.207.76.1   wanidle0 SG   100  8     0
20887
127.0.0.1/32      -             lo0      CP   0    0     0
20887
10.0.0.0/24        10.0.0.100     wan0     SG   100   1
21387 20887
10.0.0.100/32     10.0.0.100     wan0    S   100  1    153
20887
10.1.2.0/24        -              ie0      C    0     0
19775 20887
10.1.2.1/32        -             lo0      CP   0    0    389
20887
255.255.255.255/32 - ie0      CP   0     0     0     20887
```

Die Felder haben die folgende Bedeutung:

Destination	Zieladresse der Route. Um Pakete an diese Adresse zu senden, verwendet die Pipeline diese Route. Beachten Sie, daß der Router stets die am genauesten angegebene Route (die Route mit der größten Netzmaske) zum jeweiligen Ziel verwendet.
Gateway	Adresse des Routers für den höchsten Hop, der Pakete an die angegebene Adresse weiterleiten kann. Bei direkten Routen (ohne Gateway) erscheint in der Spalte „Gateway“ keine Gateway-Adresse.

IF	„ie0“ steht für die Ethernet-Schnittstelle, „lo0“ steht für die Rückschleifen-Schnittstelle, „wanN“ gibt die einzelnen aktiven WAN-Schnittstellen in der Reihenfolge an, in der sie aktiv wurden, und „wanidle0“ ist die inaktive Schnittstelle (die Schnittstelle, zu der alle Pakete umgeleitet werden, wenn die WAN-Verbindungen der jeweiligen Routen unterbrochen sind).
Flg	Eines der folgenden Zeichen: • C – „Connected“ (direkt verbundene Route, z. B. das Ethernet) • I – ICMP (dynamische ICMP-Redirect-Route) • N – „NetMgt“ (über SNMP-MIB II in die Tabelle aufgenommen) • R – RIP (dynamische RIP-Route) • S – „Static“ (lokal in einem IP-Routing- oder Verbindungsprofil konfigurierte Route) • ? – Unbekannt (Route mit unbekanntem Fehler; zeigt einen Fehler an) • G – „Gateway“ (diese Route kann nur über ein Gateway erreicht werden) • P – „Private“ (diese Route wird nicht über RIP bekanntgemacht) • T – „Temporary“ (diese Route wird zerstört, wenn ihre Schnittstelle nicht mehr verfügbar ist) • * – verborgen (Wenn eine Route verborgen ist, heißt das, daß es eine bessere Route in der Tabelle gibt, so daß diese Route „hinter“ der besseren Route verborgen ist. Ist die bessere Route nicht mehr verfügbar, kann statt dessen diese Route verwendet werden.)
Pref	Präferenzwert für die Route. Alle Routen, die über RIP in die Tabelle aufgenommen wurden, haben den Präferenzwert „100“, während der Präferenzwert für individuelle statische Routen einzeln festgelegt werden kann.
Met	RIP-Metrik für die Route; gültiger Wertebereich: 0 bis 16
Use	Angabe, wie oft die Route seit ihrer Erstellung verwendet wurde (viele dieser Zugriffe laufen intern ab, so daß aus diesem Wert nicht auf die Anzahl der Pakete geschlossen werden kann, die über die Route gesendet wurden)
Age	Alter der Route in Sekunden; anhand dieses Wertes lassen sich Probleme erkennen, wenn Routen sich schnell ändern oder „flattern“

UDP-Statistiken

Wenn Sie sich die Anzahl der gesendeten und empfangenen UDP-Pakete (User Datagram Protocol) anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show udp stats
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
22386 packets received.
    0 packets received with no ports.
    0 packets received with errors.
    0 packets dropped
    9 packets transmitted.
```

Informationen zum UDP-Port

Wenn Sie sich Informationen über die Socket-Nummer, die UDP-Portnummer und die Nummer der Pakete in den Warteschlangen der einzelnen UDP-Ports anzeigen lassen wollen, auf denen die Pipeline gegenwärtig empfangsbereit ist, ist der folgende Befehl einzugeben:

```
ascend% show udp listen
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Socket       Local Port      InQLen
     0             520           0
     1               7           0
     2             123           0
     3             514           0
     4             161           0
     5             162           0
```

Die Felder haben die folgende Bedeutung:

Socket	Socket-Nummer für den Port
Local Port	UDP-Port, auf dem die Pipeline empfangsbereit ist
InQLen	Eingangswarteschlange für den jeweiligen Port

TCP-Statistiken

Wenn Sie sich die Anzahl der gesendeten und empfangenen TCP-Pakete (Transmission Control Protocol) anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show tcp stats
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
        0 active opens.
       11 passive opens.
        1 connect attempts failed.
        1 connections were reset.
        3 connections currently established.
    85262 segments received.
    85598 segments transmitted.
      559 segments re-transmitted.
```

Mit „active open“ werden offene TCP-Sitzungen bezeichnet, die von der Pipeline initiiert wurden. „Passive opens“ sind offene TCP-Sitzungen, die nicht von der Pipeline initiiert wurden.

Informationen zur TCP-Verbindung

Wenn Sie sich die aktuellen TCP-Sitzungen der Pipeline (sowohl ankommend als auch abgehend) anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show TCP connection
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Socket       Local              Remote
   State
0            *.23               *.*
  LISTEN
1            10.2.3.23          15.5.248.121.15003   EST
ABLISHED
```

Die Felder haben die folgende Bedeutung:

Socket	Socket-Nummer des Ports
Local	lokale IP-Adresse und Port der Verbindung; wenn die Pipeline z. B. eine Verbindung mit einem lokalen Host mit der Adresse 10.0.0.2 über Port 23 hat, wird unter „Local“ „10.0.0.2.23“ angegeben
Remote	IP-Adresse und Port des entfernten Geräts, von dem die Verbindung initiiert wurde; wenn die Verbindung z. B. von der Adresse 200.5.248.210 am Port 18929 ausging, wird unter „Remote“ „200.5.248.210.18929“ angegeben
State	entweder „LISTEN“, wenn die Pipeline für eine Verbindung empfangsbereit ist, oder „ESTABLISHED“, wenn bereits eine Verbindung besteht

Anzeigen von NetWare-Informationen

In diesem Abschnitt wird beschrieben, wie Sie sich Informationen über die IPX-Pakete sowie den Inhalt der IPX-Routing- und Server-Tabellen anzeigen lassen können.

IPX-Statistiken

Wenn Sie sich statistische Informationen über die gesendeten und empfangenen IPX-Pakete anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show netware stats
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
27162 packets received.
25392 packets forwarded.
0 packets dropped exceeding maximum hop count.
0 outbound packets with no route.
```

Die Pipeline sondert Pakete aus, die den maximalen Hop-Wert überschreiten, also bereits zu viele Router passiert haben.

Informationen zu den angebotenen IPX-Diensten

Wenn Sie sich die IPX-Server-Tabelle anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show netware servers
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
IPX address                    type            server
name
ee000001:000000000001:0040     0451            server-
1
```

Die Felder haben die folgende Bedeutung:

IPX address	IPX-Adresse des Servers; Format: <Netzwerknummer>:<Knotennummer>:<Socket-Nummer>
type	verfügbarer Diensttyp (im hexadezimalen Format); z. B. steht „0451“ für einen Dateiserver
server name	die ersten 35 Zeichen des Servernamens

Informationen zum IPX-Routing

Wenn Sie sich Informationen zur IPX-Routing-Tabelle anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show netware networks
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
network     next router        hops        ticks   origin
CFFF0001    00000000000         0          1       Ethern
et         S
```

Die Felder haben die folgende Bedeutung:

network	IPX-Netzwerknummer
next router	Adresse des nächsten Routers; bei WAN-Verbindungen 0 (Null)

hops	Hop-Wert zum Netzwerk
ticks	Tick-Wert zum Netzwerk
origin	Name des Profils für den Zugang zum Netzwerk

Hinweis: Neben dem „origin“-Wert kann entweder ein „S“ oder ein „H“ erscheinen. „S“ steht für statische Routen und „H“ für verborgene („hidden“) statische Routen. Verborgene statische Routen gibt es dann, wenn der Router von einer besseren Route erfährt.

IPXPING-Statistiken

Wenn Sie sich statistische Informationen im Zusammenhang mit dem Befehl „IPXPING“ anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show netware pings
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
InPing Requests/OutPing Replies OutPing Requests/InPing
Replies
      10            10                  18            18
```

Aus dieser Anzeige läßt sich erkennen, wie viele NetWare-Stationen die Pipeline „gepingt“ haben (InPing-Anforderungen und -Antworten), und wie oft der Befehl „IPXPING“ in der Pipeline verwendet wurde. Siehe dazu „Überprüfen der Bereitschaft eines NetWare-Systems mit dem Befehl „IPXPING““ auf Seite 11-61.

Anzeigen der ISDN-Informationen

Mit dem Befehl „SHOW ISDN“ können Sie sich die letzten 20 Ereignisse anzeigen lassen, die am angegebenen ISDN-Anschluß eingetreten sind. Zur Eingabe des Befehls ist das folgende Format zu verwenden:

```
show isdn <Anschlußnummer>
```

<Anschlußnummer> ist die Nummer des ISDN-Anschlusses. Um sich z. B. Informationen über den am weitesten links eingebauten WAN-Anschluß anzeigen zu lassen, ist der folgende Befehl einzugeben:

```
ascend% show isdn 0
```

Die Pipeline antwortet mit mindestens einer der folgenden Meldungen:

```
PH: ACTIVATED
PH: DEACTIVATED
DL: TEI ASSIGNED (nur bei BRI-Schnittstellen)
DL: TEI REMOVED (nur bei BRI-Schnittstellen)
NL: CALL REQUEST
NL: CLEAR REQUEST
NL: ANSWER REQUEST
NL: CALL CONNECTED
NL: CALL FAILED/T303 EXPIRY
NL: CALL CLEARED/L1 CHANGE
NL: CALL REJECTED/OTHER DEST
NL: CALL REJECTED/BAD CALL REF
NL: CALL REJECTED/NO VOICE CALLS
NL: CALL REJECTED/INVALID CONTENTS
NL: CALL REJECTED/BAD CHANNEL ID
NL: CALL FAILED/BAD PROGRESS IE
NL: CALL CLEARED WITH CAUSE
```

In einigen Fällen kann die Meldung auch eine Telefonnummer (angezeigt durch das Präfix #), einen Datendienst (mit dem Suffix K für kBit/s), eine Kanalnummer, eine TEI-Zuordnung oder einen Fehlercode enthalten. Beispiel:

```
PH: ACTIVATED
NL: CALL REQUEST: 64K, #442
NL: CALL CONNECTED: B2, #442
NL: CLEAR REQUEST: B1
NL: CALL CLEARED WITH CAUSE 16 B1 #442
```

Informationen zu den möglichen Meldungen finden Sie im CCITTT Blue Book Q.931 bzw. in anderen ISDN-Spezifikationen.

Anzeigen der Frame-Relay-Informationen

In diesem Abschnitt wird beschrieben, wie Sie sich Informationen zu Frame-Relay-Schnittstellen anzeigen lassen können.

Frame-Relay-Statistiken

Wenn Sie sich den Status der Frame-Relay-Schnittstellen anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show fr stats
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
Name          Status       Speed        MTU   InFrame
 OutFrame
framerelay      Down       56000       1532         0
        0
```

Die Felder haben die folgende Bedeutung:

Name	Name des Frame-Relay-Profils der Schnittstelle
Status	Status der Schnittstelle:
	„Up“ bedeutet, daß die Schnittstelle betriebsbereit ist, ohne dabei unbedingt gerade mit einem aktiven Ruf beschäftigt zu sein.
	„Down“ bedeutet, daß die Schnittstelle nicht betriebsbereit ist.
Speed	Datenübertragungsgeschwindigkeit in Bit/s
MTU	*Maximum Transmission Unit*: von der Schnittstelle unterstützte maximale Paketgröße
InFrame	Anzahl der von der Schnittstelle empfangenen Rahmen
OutFrame	Anzahl der von der Schnittstelle gesendeten Rahmen

DLCI-Status

Wenn Sie sich den Status der einzelnen DLCIs (Data Link Connection Identifier), die die Frame-Relay-Schnittstelle verwenden, anzeigen lassen wollen, ist der Befehl „SHOW FR DLCI“ im folgenden Format einzugeben:

```
show fr dlci <Profilname>
```

<Profilname> steht für den Namen eines Frame-Relay-Profils. Beispiel:

```
ascend% show fr dlci PacBell
```

Wenn Sie diesen Befehl eingeben, werden der Name des Frame-Relay-Profils, eine Liste aller Verbindungsprofile, die die jeweiligen DLCIs verwenden und statistische Angaben über diese DLCIs angezeigt. Zur Angabe der DLCI-Informationen für die einzelnen Verbindungsprofile werden die folgenden Felder verwendet:

Informationen zur Verbindungsverwaltung

Wenn Sie sich Informationen zur Verbindungsverwaltung (Link Management Information, LMI) für jede vom Frame-Relay-Profil aktivierte Verbindung anzeigen lassen wollen, ist der folgende Befehl einzugeben:

```
ascend% show fr lmi
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
LMI for name:
   Invalid Unnumbered info      0    Invalid Prot
Disc        0
   Invalid dummy call Ref       0    Invalid Msg
Type         0
   Invalid Status Message       0    Invalid Lock
Shift       0
   Invalid Information ID       0    Invalid Report
Type      0
   Num Status Enq. Sent         0    Num Status msgs
Rcvd     0
   Num Update Status Rcvd       0    Num Status
Timeouts      0
```

Diese Informationen beruhen auf dem lokalen Inkanal-Zeichengabeprotokoll gemäß ANSI T1.617 Anhang D. (Eine ausführliche Beschreibung der Felder dieser Anzeige können Sie Anhang D entnehmen.)

Anzeigen der Betriebszeit des Systems

Wenn Sie sich anzeigen lassen wollen, wie lange die Pipeline seit dem letzten Einschalten bzw. Zurücksetzen bereits in Betrieb ist, ist der folgende Befehl einzugeben:

```
ascend% show uptime
```

Auf dem Bildschirm erscheint daraufhin die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
system uptime: up 2 days, 4 hours, 38 minutes, 43 seconds
```

Wenn die Pipeline 1000 aufeinanderfolgende Tage durchgängig in Betrieb bleibt, beginnt die Zählung der Tage wieder bei 0.

Hinzufügen und Löschen von IP-Routen

Sie können sich die Routing-Tabelle nicht nur anzeigen lassen, sondern auch mit Hilfe von Terminal-Server-Befehlen der Tabelle Routen hinzufügen bzw. Routen aus der Tabelle löschen.

Hinweis: Der Befehl „IPROUTE SHOW“ hat die gleiche Wirkung wie der Befehl „SHOW IPROUTES“. Informationen dazu, welche Angaben Sie sich mit diesem Befehl anzeigen lassen können, finden Sie im Abschnitt „Informationen zum IP-Routing“ auf Seite 11-45.

Hinzufügen von statischen Routen

Wenn Sie der Routing-Tabelle der Pipeline eine statische Route hinzufügen wollen, ist der Befehl „IPROUTE ADD“ einzugeben. Dabei ist das folgende Format zu verwenden:

```
iproute add <Ziel/Größe><Gateway>[Präferenz]
[Metrik][Protokoll]
```

Argumente des Befehls „iproute add“

Der Befehl „IPROUTE ADD“ hat die folgenden Argumente:

- Ziel/Größe

  Hiermit wird die Netzwerkadresse und die Subnetzmaske in der Ascend-Netzmaskennotation angegeben. Weitere Informationen zu den Subnetzmasken finden Sie im Abschnitt „Die Ascend-Netzmaskenkonvention“ auf Seite 7-5.

- Gateway

  Hiermit wird die IP-Adresse des Routers angegeben, der Pakete zu diesem Netzwerk weiterleiten kann.

- Präferenz

  Dies ist der Präferenzwert für die Route. Bei der Bestimmung, welche Routen in die Routing-Tabelle aufgenommen werden sollen, vergleicht der Router zunächst die Präferenzwerte und wählt die niedrigere Nummer. Sind die Präferenzwerte gleich, vergleicht der Router als nächstes die Metrikwerte und entscheidet sich für die Route mit der niedrigeren Metrik.

- Metrik

  Dies ist der virtuelle Hop-Wert zum Zielnetzwerk (Standard 7).

- Protokoll

  Hiermit wird das Protokoll der Route angegeben.

Beispiel:

```
ascend% iproute add 10.1.2.0 10.0.0.3/24 1
```

Mit diesem Befehl wird der IP-Routing-Tabelle eine Route zum Netzwerk 10.1.2.0 und all seinen Subnetzen durch den IP-Router mit der Adresse 10.0.0.3/24 hinzugefügt. Die Metrik zur Route hat einen Wert von 1 (d. h., die Route ist ein Hop entfernt).

Wenn Sie versuchen, eine Route zu einem Ziel hinzuzufügen, das in der Routing-Tabelle bereits existiert, ersetzt die Pipeline die bestehende Route, jedoch nur dann, wenn diese eine höhere Metrik hat. Wird die Meldung „Warning: a better route appears to exist“ angezeigt, hat die Pipeline Ihren Versuch, eine Route hinzuzufügen, abgewiesen, da die Routing-Tabelle diese

Route bereits mit einer niedrigeren Metrik enthielt. Beachten Sie, daß sich die Metrik für eine Route durch eine RIP-Aktualisierung ändern kann.

Hinweis: Der Befehl „IPROUTE ADD“ fügt eine statische Route hinzu, die beim Zurücksetzen der Pipeline verlorengeht. Nähere Informationen zum IP-Routing entnehmen Sie bitte dem Kapitel 7, „Konfigurieren der Pipeline als IP-Router“.

Löschen von Routen

Wenn Sie eine Route aus der Routing-Tabelle der Pipeline löschen wollen, ist der Befehl „IPROUTE DELETE“ einzugeben. Dabei ist das folgende Format zu verwenden:

```
iproute delete <Ziel/Größe><Gateway>[Protokoll]
```

Beispiel:

```
ascend% iproute delete 10.1.2.0 10.0.0.3/24
```

Hinweis: Durch RIP-Aktualisierungen können alle von Ihnen mit „IPROUTE DELETE“ gelöschten Routen wieder hinzugefügt werden. Außerdem stellt die Pipeline nach jeder Zurücksetzung des Systems automatisch alle Routen im „Static Rtes“-Profil wieder her.

Argumente des Befehls „iproute delete“

Der Befehl „IPROUTE DELETE“ hat die folgenden Argumente:

- Ziel/Größe
  Hiermit wird die Ziel-Netzwerkadresse angegeben.
- Gateway
  Hiermit wird die IP-Adresse des Routers angegeben, der Pakete zu diesem Netzwerk weiterleiten kann.
- Protokoll
  Hiermit wird das Protokoll der Route angegeben.

Überprüfen der Bereitschaft eines IP-Hosts mit dem Befehl „PING“

Der Befehl „PING“ sendet ein ICMP-Datagramm mit obligatorischer Echoanforderung (echo_request), das bei der entfernten Station anfragt: „Bist du da?“ Wenn die entfernte Station die Echoanforderung empfängt, sendet sie ein ICMP-Echoantwort-Datagramm (echo_response) zurück, in dem dem Sender mitgeteilt wird „Ja, ich bin da und bereit.“ Durch diesen Nachrichtenaustausch wird überprüft, ob der Übertragungsweg zwischen der Pipeline und der anderen Station offen ist.

Der Befehl „PING“ hat das folgende Format:

```
ping [-qv] [-c Anzahl Pakete] [-i Verzögerung] [-s Paket-
größe] Hostname
```

Beispiel:

```
ascend% ping -c 256 10.1.2.3
```

Sie können den PING-Nachrichtenaustausch mit Hilfe der Tastenkombination Strg-C jederzeit abbrechen. Während des PING-Nachrichtenaustauschs erscheint auf dem Bildschirm ungefähr die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
PING 10.1.2.3 (10.1.2.3): 56 data bytes
64 bytes from 10.1.2.3: icmp_seq=0 ttl=255 time=30 ms
64 bytes from 10.1.2.3: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 10.1.2.3: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 10.1.2.3: icmp_seq=3 ttl=255 time=10 ms
64 bytes from 10.1.2.3: icmp_seq=4 ttl=255 time=0 ms
^ C
--- 10.1.2.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/1/30 ms
```

Es werden die folgenden Informationen angezeigt:

- TTL-Wert (Time-To-Live) für jedes der ICMP-ECHO_RESPONSE-Datagramme

  Der maximale TTL-Wert für ICMP-PING-Datagramme ist 255, und der maximale TTL-Wert für TCP liegt häufig bei 60 oder darunter. Daher kann es passieren, daß Sie einen Host zwar „pingen“ können, ihn aber nicht mit einer TCP-Anwendung (wie z. B. Telnet oder FTP) erreichen.

  Wenn Sie einen Host „pingen“, der mit einer Berkeley-UNIX-Version vor 4.3BSD-Tahoe arbeitet, ist der TTL-Wert 255 minus der Anzahl der Router auf dem Weg zum Host und von dort zurück. Bei Hosts, auf denen die aktuelle Version von Berkeley UNIX läuft, ist der TTL-Wert 255 minus der Anzahl der Router auf dem Weg vom entfernten System zur Station, von der aus „PING“ aufgerufen wurde.
- doppelt vorhandene bzw. beschädigte ECHO_RESPONSE-Pakete
- Umlaufzeit und Angaben zu Paketverlusten

  In einigen Fällen kann die Umlaufzeit nicht berechnet werden.

Argumente des Befehls „PING“

Der Befehl „PING“ hat die folgenden Argumente:

- Hostname

  IP-Adresse oder Name des Hosts
- [-q]

  (Optional) Stumme („quiet“) Eingabe. Bis auf die zusammenfassenden Zeilen am Anfang und Ende des Befehls werden keine weiteren Informationsmeldungen angezeigt.
- [-v]

  (Optional) Ausgabe mit Meldungsanzeige („verbose“). Die Pipeline listet alle empfangenen ICMP-Pakete, mit Ausnahme der ECHO_RESPONSE-Pakete, auf.
- [-c Anzahl Pakete]

  (Optional) Der Test soll nach dem Senden und Empfangen der angegebenen Zahl von Paketen gestoppt werden.

- [-i Verzögerung]
  (Optional) Es soll die angegebene Zahl von Sekunden gewartet werden, bevor das nächste Paket gesendet wird. Der Standardwert ist 1 Sekunde.
- [-s Paketgröße]
  (Optional) Es soll die angegebene Anzahl von Datenbytes gesendet werden. Der Standardwert ist 56 Byte. Die Paketgröße beinhaltet nicht den 8-Byte-ICMP-Header.

Überprüfen der Bereitschaft eines NetWare-Systems mit dem Befehl „IPXPING“

Mit Hilfe des Befehls „IPXPING“ können Sie den Übertragungsweg zu NetWare-Stationen in der Netzwerkschicht überprüfen. Er kann sowohl im selben LAN wie die Pipeline als auch über WAN-Verbindungen eingesetzt werden, bei denen das IPX-Routing aktiviert ist.

Zur Eingabe des Befehls „IPXPING“ ist das folgende Format zu verwenden:

```
ipxping [-c Anzahl Pakete] [-i Verzögerung] [-s
Paketgröße] <[Servername]
[Netznummer:Knotennummer]>
```

<Servername> ist entweder die IPX-Adresse der NetWare-Workstation oder der bekanntgemachte Name eines Servers.

Die IPX-Adresse besteht aus der IPX-Netzwerk- und Knotennummer einer Station. Beispiel:

```
ascend% ipxping CFFF1234:000000000001
```

Wenn Sie mit „IPXPING“ die Verbindung zu einem bekanntgemachten NetWare-Server überprüfen wollen, brauchen Sie nur den symbolischen Namen des Servers einzugeben. Beispiel:

```
ascend% ipxping server-1
```

Durch Drücken von Strg-C können Sie die Ausführung von „IPXPING“ jederzeit abbrechen.

Während des IXPING-Nachrichtenaustauschs erscheint auf dem Bildschirm ungefähr die folgende Anzeige (die angegebenen Werte sind Beispielwerte):

```
PING server-1 (EE000001:000000000001): 12 data bytes
52 bytes from (EE000001:000000000001): ping_id=0 time=0ms
52 bytes from (EE000001:000000000001): ping_id=1 time=0ms
52 bytes from (EE000001:000000000001): ping_id=2 time=0ms
?
--- novl1 Ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Es werden im einzelnen die folgenden Informationen angezeigt:

- die IPX-Adresse des Ausgangs- und des Zielknotens
- die Anzahl der Bytes in den angeforderten und zurückgesendeten Paketen
- die PING-Kennung („ping_id“) des Befehls (die PING-Anforderungsnummer, auf die der Zielhost geantwortet hat)
- die Zeit (in Millisekunden), die für das Senden des IPXPING-Befehls und das Empfangen einer Antwort erforderlich ist
- die Anzahl der gesendeten und empfangenen Pakete
- doppelt vorkommende und beschädigte Pakete, falls vorhanden
- mittlere Umlaufzeit für die PING-Anforderung und die Antwort
  In einigen Fällen können die Umlaufzeiten nicht berechnet werden.

Argumente des Befehls „IPXPING“

Der Befehl „IPXPING“ hat die folgenden Argumente:

- Servername
  Der bekanntgemachte Name des IPX-Servers.
- [-c Anzahl Pakete]
  (Optional) Der Test soll nach dem Senden und Empfangen der angegebenen Zahl von Paketen gestoppt werden.
- [-i Verzögerung]
  (Optional) Es soll die angegebene Zahl von Sekunden gewartet werden, bevor das nächste Paket gesendet wird. Der Standardwert ist 1 Sekunde.
- [-s Paketgröße]

(Optional) Es soll die angegebene Anzahl von Datenbytes gesendet werden. Der Standardwert ist 56 Byte. Die Paketgröße beinhaltet nicht den 8-Byte-ICMP-Header.

- [Netznummer:Knotennummer]

  Die IPX-Netzwerk- und Knotennummer eines IPX-Hosts.

  – Die Netzwerknummer kann zwischen 0x00000000 (lokales Netzwerk) und 0xfffffffe liegen.

  – Die Knotennummer kann zwischen 0x0000000001 und 0xfffffffffe liegen.

Anmelden bei einem IP-Host mit dem Befehl „TELNET“

Mit dem Befehl „TELNET“ können Sie sich bei einem entfernten Host anmelden („einloggen“). Dabei ist das folgende Format zu verwenden:

```
telnet [-a|-b] <Hostname> [<Portnummer>]
```

Im Ethernet-Profil gibt es eine Reihe von Einstellungen, die sich auf den Telnet-Betrieb auswirken. Wenn z. B. DNS konfiguriert ist, können Sie einen Hostnamen angeben. Beispiel:

```
ascend% telnet meinhost
```

Wurde DNS nicht konfiguriert, müssen Sie statt dessen die IP-Adresse des Hosts angeben.

Eine andere Möglichkeit, eine Sitzung zu öffnen, besteht darin, zunächst den Befehl „TELNET“ aufzurufen und dann an der Telnet-Eingabeaufforderung den Befehl „OPEN“ einzugeben. Beispiel:

```
ascend% telnet
telnet> open meinhost
```

In den Beispielen in diesem Abschnitt besteht die Telnet-Eingabeaufforderung aus dem Wort „telnet“ und einem Größer-als-Zeichen („telnet>“). Wenn Sie diese Eingabeaufforderung sehen, können Sie jeden der im Abschnitt „Befehle für Telnet-Sitzungen“ auf Seite 11-65 beschriebenen Telnet-Befehle eingeben.

Hinweis: Wenn bereits eine Telnet-Verbindung besteht, können Sie die Eingabeaufforderung „telnet>“ und die Telnet-Befehlszeilenschnittstelle aufrufen, indem Sie die Tastenkombination Strg-] drücken. Mit jedem gültigen Telnet-Befehl kehren Sie wieder zur offenen Sitzung zurück. Beachten Sie, daß die Tastenkombination Strg-] im binären Telnet-Modus nicht funktioniert. Wenn Sie über Telnet auf die Pipeline zugreifen, empfiehlt es sich daher, für die Escape-Sequenz etwas anderes als Strg-] einzustellen.

Sie können die Telnet-Sitzung jederzeit verlassen, indem Sie an der Telnet-Eingabeaufforderung den folgenden Befehl eingeben:

```
telnet> quit
```

Argumente des Befehls „TELNET“

Der Befehl „TELNET“ hat die folgenden Argumente:

- <Hostname>

  Wenn DNS konfiguriert wurde, können Sie den Hostnamen des entfernten Systems angeben. Andernfalls ist für <Hostname> die IP-Adresse der entfernten Station anzugeben.

- [–a]

  (Optional) Mit diesem Flag wird der Standard-7-Bit-Modus festgelegt, bei dem Bit 8 den Wert 0 hat. 7-Bit-Telnet wird auch als NVT-ASCII (Network Virtual Terminal) bezeichnet. Wenn Sie weder –a noch –b eingeben, gilt die Binärmodus-Einstellung.

- [–b]

  (Optional) Mit diesem Flag wird der Telnet-8-Bit-Binärmodus festgelegt. Dieser Modus wird für X-Modem und andere 8-Bit-Dateitransferprotokolle benötigt. Wenn Sie weder –a noch –b eingeben, gilt die Binärmodus-Einstellung.

Hinweis: Beachten Sie, daß die Telnet-Escape-Sequenz nicht im 8-Bit-Binärmodus arbeitet. Die Telnet-Sitzung kann nur geschlossen werden, wenn ein Ende der Verbindung die Sitzung beendet. Daher haben lokale Benutzer, die nicht über eine Wählverbindung verbunden sind, keine Möglichkeit, die Sitzung von sich aus zu schließen. In diesem Fall muß gewartet werden, bis der entfernte Benutzer die Sitzung schließt.

- [<Portnummer>]
  (Optional) Hiermit können Sie festlegen, welcher Port für die Sitzung verwendet werden soll. Der Standardwert ist „23“, der üblicherweise für Telnet verwendete Port.

Befehle für Telnet-Sitzungen

Die in diesem Abschnitt beschriebenen Befehle können während einer offenen Sitzung an der Telnet-Eingabeaufforderung eingegeben werden. Die Telnet-Eingabeaufforderung wird während einer aktiven Verbindung zum angegebenen Host aufgerufen, wenn Sie die Tastenkombination Strg-] drücken.

Wenn Sie Informationen zu den Befehlen für Telnet-Sitzungen benötigen, geben Sie den Befehl „HELP“ bzw. „?“ ein. Beispiel:

```
telnet> ?
```

bzw.

```
telnet> help
```

Zum Öffnen einer Telnet-Verbindung nach Verwendung des Befehls „TELNET“ steht der Befehl „OPEN“ zur Verfügung. Die Argumente dieses Befehls sind mit denen identisch, die Sie zum Öffnen einer Verbindung von der TELNET-Befehlszeile aus verwenden; die einzige Ausnahme ist, daß der Befehl „OPEN“ nicht die Optionen “-a“ und “-b“ unterstützt. Siehe dazu „Argumente des Befehls „TELNET““ auf Seite 11-64. Beispiel:

```
telnet> open meinhost
```

Zum Senden von Standard-Telnet-Befehlen, wie „Are You There“ oder „Suspend Process“, ist der Befehl „SEND“ zu verwenden. Beispiel:

```
telnet> send susp
```

Eine Liste der „SEND“-Befehle und der mit ihnen zusammenhängenden Befehlssyntax wird angezeigt, wenn Sie den folgenden Befehl eingeben:

```
telnet> send ?
```

Zur Festlegung von Sonderzeichen für die Verwendung während der Telnet-Sitzung können Sie den Befehl „SET“ verwenden. Beispiel:

```
telnet> set eof ^D
```

Die gegenwärtigen Einstellungen lassen sich mit dem folgenden Befehl anzeigen:

```
telnet> set all
```

Eine Aufstellung aller SET-Befehle erhalten Sie über den Befehl:

```
telnet> set ?
```

Wenn Sie die Telnet-Sitzung verlassen und die Verbindung schließen wollen, können Sie den Befehl „CLOSE“ bzw. „QUIT“ verwenden. Beispiel:

```
telnet> close
```

oder:

```
telnet> quit
```

TELNET-Fehlermeldungen

Die Pipeline gibt für jeden Zustand, der zum Nichtzustandekommen einer Telnet-Sitzung oder zu deren vorzeitigem Abbruch führt, eine Fehlermeldung aus. Folgende Fehlermeldungen können angezeigt werden:

`no connection: host reset`	Der Ziel-Host hat die Verbindung zurückgesetzt.
`no connection: host unreachable`	Der Ziel-Host ist nicht erreichbar.
`no connection: net unreachable`	Das Ziel-Netzwerk ist nicht erreichbar.
`Unit busy. Try again later.`	Es wurde die Höchstzahl der gleichzeitig ablaufenden Telnet-Sitzungen erreicht.

Öffnen einer reinen TCP-Verbindung zu einem IP-Host

Mit dem Befehl „TCP“ können Sie sich bei einem entfernten Host anmelden. Dabei ist das folgende Format zu verwenden:

```
tcp <Hostname> <Portnummer>
```

Im Ethernet-Profil gibt es eine Reihe von Einstellungen, die sich auf den Betrieb der TCP-Verbindung auswirken. Wenn z. B. im Ethernet-Profil der Pipeline DNS konfiguriert ist, können Sie einen Hostnamen angeben. Beispiel:

```
ascend% tcp meinhost
```

Argumente des Befehls „TCP“

Der Befehl „TCP“ hat die folgenden Argumente:

- <Hostname>

  Wenn im Ethernet-Profil der Pipeline DNS konfiguriert wurde, können Sie den Hostnamen des entfernten Systems angeben. Andernfalls muß für <Hostname> die IP-Adresse der entfernten Station angegeben werden.

- [<Portnummer>]

  (Optional) Hiermit können Sie angeben, welchen Port die Sitzung verwenden soll. Die Portnummer gibt im Normalfall eine benutzerdefinierte Anwendung an, die über der TCP-Sitzung läuft. So wird z. B. mit der Portnummer 23 eine Telnet-Sitzung gestartet. Durch das Beenden der Telnet-Sitzung wird jedoch nicht auch gleichzeitig die reine TCP-Sitzung beendet.

Wenn die TCP-Sitzung zu arbeiten beginnt, zeigt die Pipeline das Wort „connected“ an. Sie können die TCP-Sitzung nun zum Datentransport verwenden, indem Sie eine entsprechende Anwendung über der TCP-Sitzung laufen lassen.

Die reine TCP-Sitzung kann von beiden Seiten der Verbindung aus durch Aufhängen beendet werden. Bei der Beendigung einer Sitzung zu einem entfernten Terminal-Server wird auch die TCP-Sitzung beendet.

TCP-Fehlermeldungen

Wenn es nicht gelingt, eine reine TCP-Verbindung aufzubauen, gibt die Pipeline eine der folgenden Fehlermeldungen aus:

`Can’t open session: <Hostname> <Portnummer>`	Es wurde ein ungültiger oder unbekannter Wert für <Hostname> oder <Portnummer> eingegeben oder die Portnummer fehlt völlig.
`no connection: host reset`	Der Ziel-Host hat die Verbindung zurückgesetzt.
`no connection: host unreachable`	Der Ziel-Host ist nicht erreichbar.
`no connection: net unreachable`	Das Ziel-Netzwerk ist nicht erreichbar.

Technische Spezifikationen

A

In diesem Anhang werden die Spezifikationen für verschiedene Facetten der Pipeline beschrieben und die Anforderungen an die Kabel erläutert. Der Anhang enthält die folgenden Abschnitte:

Allgemeine Spezifikationen

Stromversorgung

Die Anforderungen an die Stromversorgung der Pipeline werden in Tabelle A-1 aufgeführt.

Tabelle A-1: Anforderungen an die Stromversorgung der Pipeline

Element	Wert
Spannung	90–130 V AC, 0,4 A 47–63 Hz 220–240 V AC, 0,2 A 47–63 Hz
Phase	einphasig
Frequenz	47–63 Hz
Leistung	11 W (nominell) bis 13,5 W (maximal)

Die Pipeline-Konfigurationsprofile werden in einem batteriebetriebenen Speicher gespeichert, so daß sie beim Ausschalten der Pipeline nicht verlorengehen.

Hinweis: Verwenden Sie eine geschützte Wechselstromquelle bzw. schalten Sie zwischen Stromquelle und Pipeline einen Überspannungsschutz.

Anforderungen an die Betriebsumgebung

Um einen optimalen Betrieb der Pipeline zu gewährleisten, sollte die Pipeline in einem Raum mit gleichbleibender Temperatur und Luftfeuchtigkeit aufgestellt werden. Allgemein gilt, daß kühlere Umgebungsbedingungen besser sind. Für den Betrieb wird eine Raumtemperatur zwischen 0 ˚C und 40 ˚C empfohlen.

Die Luftfeuchtigkeit sollte so hoch sein, daß es nicht zu einer Ansammlung statischer Elektrizität kommt, aber auch niedrig genug, um Kondensation zu vermeiden. Beim Betrieb ist eine relative Luftfeuchtigkeit von maximal 90 % (nicht kondensierend) akzeptabel.

Die Pipeline kann in Höhenlagen zwischen 0 und 4500 m betrieben werden.

Spezifikationen zur Benutzerschnittstelle

In diesem Abschnitt finden Sie Informationen zur Anschlußbelegung der „Terminal“-Anschlußschnittstelle.

„Terminal“-Anschluß und Anschlußbelegung

Der „Terminal“-Anschluß verwendet eine Standard-DE-9-Buchse, die dem EIA-RS-232-Standard für serielle Schnittstellen entspricht.

Alle Pipeline-Modelle verwenden die in Table A-2 beschriebene RS-232-Anschlußbelegung.

Tabelle A-2: Steckerbelegung für den „Terminal“-Anschluß

DE-9-Stift	RS-232-Signal	Funktion	E/A
1	DCD	Data Carrier Detect	A
2	RD	Serial Receive Data	A
3	SD	Serial Transmit Data	E
4	DTR	Data Terminal Ready	E
5	GND	Signal Ground	
6	DSR	Data Set Ready	A
7	RTS	Request to Send	E
8	CTS	Clear to Send	A
*9	*RI	*Ring Indicator	*A

*Stift 9 ist nicht aktiv („Ring Indicator“-Signal wird nicht bereitgestellt).

Hinweis: Wenn Sie den seriellen Anschluß als WAN-Anschluß verwenden, wird als Zeichengabeprotokoll für den seriellen WAN-Anschluß V.35 verwendet.

Da die elektrische Schnittstelle jedoch RS-232-konform ist, muß das elektrische Signal von RS-232 zu V.35 umgewandelt werden.

Spezifikationen für die Ethernet-Schnittstelle

Die Pipeline unterstützt die physikalischen Spezifikationen gemäß IEEE l802.3 mit Ethernet 2-Framing (Ethernet/DIX). Sie verfügt über eine Ethernet-Schnittstelle und bietet Unterstützung für die folgenden Ethernet-Typen:

- Koax: Thin Ethernet und IEEE 802.3 (10Base-2) mit BNC-Stecker

Hinweis: Die Pipeline ist nicht mit einer Koax-Ethernet-Schnittstelle ausgerüstet.

- 10Base-T (UTP): Twisted-Pair-Ethernet und IEEE 802.3 (10Base-T) mit RJ-45-Stecker
- AUI (Attachment Unit Interface): Standard Ethernet und IEEE (10Base-5) mit 15poligem AUI-Stecker

Erforderliche Ausrüstungsteile

Zur Installation der Ethernet-Schnittstelle benötigen Sie die in den folgenden Abschnitten beschriebenen Ausrüstungsteile.

Koax

Sie brauchen einen BNC-T-Stecker. Wenn sich Ihre Verbindung am Ende eines Kabelsegments befindet, benötigen Sie darüber hinaus auch einen 50-Ohm-Terminator.

Zur Installation ist der LAN-BNC-T-Stecker mit dem BNC-Anschluß an der Rückseite der Pipeline zu verbinden. Als Kabel ist ein Standard-10Base-250-Ohm-Kabel, wie z. B. RG-58 A/U oder RG58 C/U, zu verwenden.

Achtung: Die Unterbrechung der Kontinuität des LAN durch Einfügen eines Kabelsegments oder Entfernen eines der 50-Ohm-Terminatoren führt zu einer Unterbrechung des Ethernet-Betriebs.

10Base-T

Sie benötigen ein Twisted-Pair-Ethernet-Kabel und ein Dual-Twisted-Pair-Kabel mit modularen RJ-45-Buchsen.

Als Kabel ist ein EIA/TIA-568- oder IEEE-802.3-10Base-T-Kabel zu verwenden. Für einige Installationen wird ein Crossover-Kabel benötigt. Dies ist z. B. dann der Fall, wenn eine direkte Verbindung zum Ethernet-Anschluß eines PC hergestellt werden soll.

AUI

Es wird ein Transceiver und ein Transceiver-Kabel benötigt.

Fehlersuche und -beseitigung

B

Dieser Anhang enthält die folgenden Abschnitte:

In diesem Anhang werden einige der am häufigsten auftretenden Probleme beschrieben, Hinweise zu deren Diagnose gegeben und Vorschläge zur Lösung gemacht. Wenn Sie das Problem mit diesen Hinweisen und Anweisungen nicht aus der Welt schaffen können, finden Sie im Kapitel 11, „Systemadministration“ weitere diesbezügliche Informationen.

Probleme mit der Verkabelung: Bitte als erstes überprüfen!

Wenn es Ihnen nicht gelingt, eine Verbindung mit einem entfernten Netzwerk herzustellen, ist als erstes zu überprüfen, ob das ISDN-Leitungskabel mit der Pipeline verbunden ist. Den Telefongesellschaften zufolge ist die fehlende Verbindung zwischen Pipeline und Telefonleitung die häufigste Ursache für anfängliche Probleme.

Ein weiteres häufiges Problem ist die falsche Ethernet-Verkabelung. Das mitgelieferte Crossover-Kabel kann nur für direkte Verbindungen zwischen dem Ethernet-Adapter (bzw. dem externen Transceiver) des Computers und der Pipeline verwendet werden. Soll die Pipeline an einen 10BaseT-Hub angeschlossen werden, muß zwischen Hub und Pipeline sowie zwischen Hub und Computer ein normales 10BaseT-Kabel verwendet werden.

Bei Macintosh-Computern kann es vorkommen, daß der Anschluß, der zum Anschließen des seriellen Kabels verwendet wird, nicht funktioniert. Sie können entweder den Modem- oder den Druckeranschluß des Macintosh-Computers verwenden. Wenn einer dieser beiden Anschlüsse nicht funktioniert, versuchen Sie es mit dem anderen.

Nähere Informationen dazu finden Sie im Abschnitt „Überprüfen der Installation“ auf Seite B-12.

Häufige Probleme und deren Lösung

In diesem Abschnitt werden Probleme beschrieben, die bei der Arbeit mit der Pipeline auftreten können, und es werden Schritte zu deren Lösung vorgeschlagen.

Allgemeine Probleme

Wenn die Liste der DO-Befehle erscheint, sind die meisten Operationen nicht verfügbar

Sie müssen u. U. ein bestimmtes „Connections“-Profil auswählen, um bestimmte DO-Befehle verwenden zu können. Wenn Sie z. B. ein „Connections“-Profil wählen wollen, müssen Sie zu diesem „Connections“-Profil im Menü „Connections“ gehen und dann Strg-D 1 eingeben.

Beachten Sie, daß Sie keine Verbindung wählen können, solange für den „Control“-Anschluß „Operations=No“ festgelegt ist. Wenn ein Ruf bereits aktiv ist, erscheint statt „DO 1 (Dial)“ der Befehl „DO 2 (Hang Up)“.

Wenn Sie die Option „DO 1 (Dial)“ nicht sehen können, kann dies mehrere Ursachen haben:

- Sie befinden sich nicht im richtigen Profil.
- Sie haben nicht die entsprechende Sicherheitsebene aktiviert.
- Im Profil wurde keine Rufnummer angegeben.
- Im Profil wurde keine IP-Adresse angegeben (wenn IP-Routing aktiviert ist).

Probleme mit der Konfiguration von Profilen

Die häufigsten Probleme sind auf falsch konfigurierte Profile zurückzuführen.

Mit dem ersten Kanal eines Invers-Multiplexing- oder MP+-Rufes kann eine Verbindung hergestellt werden, aber dann wird der Ruf beendet, oder es ist nicht möglich, auch die übrigen Kanäle zu verbinden.

Der häufigste Fehler bei der Definition von Verbindungsprofilen ist die Angabe falscher Telefonnummern. Wenn die im Verbindungsprofil der gerufenen Einheit angegebenen Telefonnummern nicht korrekt sind, ist die Pipeline nicht in der Lage, Invers-Multiplexing- oder MP+-Rufe herzustellen. Die im Verbindungsprofil angegebenen Telefonnummern sind die für Ihre Einheit lokal

zutreffenden Nummern. Geben Sie im Verbindungsprofil niemals die Nummer der Pipeline an, die gerufen wird.

Wenn die Pipeline versucht, einen Ruf zu initiieren, erscheint in der „Message Log“-Anzeige die Fehlermeldung „No Channel Avail“.

Überprüfen Sie die Konfiguration Ihres Anschlusses im „Configure“-Profil.

Probleme mit der Hardware-Konfiguration

Wenn Sie nicht über das VT-100-„Control“-Terminal mit der Pipeline kommunizieren können, kann dies daran liegen, daß ein Problem mit der Terminal-Konfiguration, dem „Control“-Anschlußkabel oder der Pipeline-Hardware vorliegt.

Auf dem VT-100-Bildschirm werden keine Daten angezeigt

In diesem Fall ist zu überprüfen, ob die Einheit alle Einschalt-Selbsttests erfolgreich abschließt. Gehen Sie dazu wie folgt vor:

1. Überprüfen Sie, ob die Pipeline und Ihr Terminal auf dieselbe Geschwindigkeit eingestellt sind.
2. Suchen Sie die LED-Anzeige „CON“.
3. Schalten Sie die Pipeline ein.

   Die LED „CON“ sollte nur während des Einschalt-Selbsttests leuchten. Wenn Sie mit dem „Control Monitor“ arbeiten, können Sie durch Drücken von Strg-L die Bildschirmanzeige aktualisieren.

   Wenn die LED „CON“ länger als eine Minute leuchten bleibt, liegt ein Problem mit der Pipeline-Hardware vor. Auch eine blinkende LED „CON“ weist auf ein Hardware-Problem hin. Wenn dies der Fall ist, setzen Sie sich am besten mit dem Ascend Customer Support in Verbindung.

Die LED „CON“ leuchtet nicht, auf dem VT-100-Terminal-Bildschirm des „Control Monitors“ werden aber auch keine Daten angezeigt.

Wenn die Einheit den Einschalt-Selbsttest erfolgreich abgeschlossen hat und Sie trotzdem nicht mit dem „Control Monitor“ kommunizieren können, sollten Sie den Bildschirm mit Strg-L aktualisieren. Werden dann immer noch keine Daten angezeigt, ist die Verkabelung zwischen der Pipeline und Ihrem Terminal zu überprüfen. Gehen Sie dazu wie folgt vor:

1 Überprüfen Sie sorgfältig die Anschlußbelegung des 9poligen Kabels.

Das „Control“-Terminal wird mit dem HHT-VT-100-Kabel bzw. dem 9poligen Anschluß mit der Beschriftung „Terminal“ an der Rückseite der Pipeline verbunden. Soll eine Verbindung zu einem IBM-PC-artigen 9poligen seriellen Anschluß hergestellt werden, kann ein einfaches Anschlußkabel verwendet werden. Andernfalls wird u. U. ein Adapterkabel benötigt, mit dem ein 9poliger Stecker mit einer 25poligen Buchse verbunden werden kann.

2 Überprüfen Sie die Einstellungen zur Flußkontrolle an Ihrem VT-100-Terminal.

Können Sie überhaupt nicht mit der Pipeline kommunizieren, ist zu überprüfen, ob die Kommunikation hergestellt werden kann, wenn alle Einstellungen zur Sende- bzw. Empfangsflußkontrolle für Ihr Terminal bzw. den Terminal-Emulator deaktiviert sind.

3 Überprüfen Sie, ob Sie einen Nullmodem-Kabelkonverter benötigen.

Im allgemeinen ist dies für die Kommunikation mit der Pipeline nicht erforderlich. Es gibt jedoch so viele verschiedene Kabel- und Terminal-Konfigurationen, daß sich in bestimmten Fällen ein Nullmodem-Kabelkonverter erforderlich macht.

Auf dem „Control Monitor“-Bildschirm erscheinen unsinnige Zeichen.

Wenn auf Ihrem Bildschirm unsinnige oder nicht lesbare Zeichen erscheinen, sind wahrscheinlich die Kommunikationseinstellungen fehlerhaft. Überprüfen Sie, ob die folgenden Einstellungen vorgenommen wurden:

- Datenübertragungsgeschwindigkeit 9600 Bits pro Sekunde
- 8 Datenbits
- 1 Stoppbit
- keine Flußkontrolle
- keine Parität

Wurde die Datenübertragungsgeschwindigkeit über das Menü „Sys Config“ geändert, ist sicherzustellen, daß auch die Einstellungen für das VT-100-Terminal entsprechend geändert werden.

Des weiteren ist sicherzustellen, daß die „Term Rate“-Einstellung der Geschwindigkeit entspricht, mit der Ihr serieller COM-Anschluß konfiguriert wurde.

Die Startanzeige meldet das Fehlschlagen eines Einschalt-Selbsttests

Wenn die Startanzeige das Fehlschlagen eines der Selbsttests beim Einschalten meldet, liegt ein interner Hardware-Fehler innerhalb der Einheit vor. Setzen Sie sich in diesem Fall mit dem Ascend Customer Support in Verbindung.

Probleme bei der Konfiguration der Pipeline

Bei der Konfiguration der Pipeline treten zwei Probleme besonders häufig auf:

- Das DFÜ-Programm zeigt kein Profil an, nachdem Strg-L gedrückt wurde.
- Nach Drücken von Strg-L erscheint zwar ein Profil, aber nicht das in diesem Handbuch dargestellte „Configure“-Profil.

Erscheinen auf dem Bildschirm unsinnige Zeichen, ist zu überprüfen, ob die VT-100-Emulation auch wirklich auf die richtige Geschwindigkeit (9600 Bits/s) eingestellt wurde.

Im DFÜ-Programm erscheint kein Profil.

Wenn nach dem Drücken von Strg-L in Ihrem DFÜ-Programm kein Profil erscheint, kann dies eine der folgenden Ursachen haben:

- Die Pipeline wird nicht mit Strom versorgt.
- Die Pipeline ist nicht mit dem seriellen Anschluß des Computers verbunden.
- Das DFÜ-Programm ist nicht ordnungsgemäß für die Pipeline konfiguriert oder es kommuniziert nicht über den richtigen Anschluß.
- Es liegt ein Hardware-Problem innerhalb der Pipeline vor.

Zur Diagnose und Lösung des Problems sind die folgenden Schritte auszuführen:

1 Überprüfen Sie die LED „PWR“ an der Frontblende der Pipeline.

Wenn die LED „PWR“ nicht leuchtet, wird die Einheit nicht mit Strom versorgt. Dies kann daran liegen, daß sie nicht mit einer Stromquelle verbunden ist. Fahren Sie mit Schritt 2 fort.

Leuchtet die LED, ist mit Schritt 4 fortzufahren.

2 Schließen Sie die Pipeline an eine Stromquelle an.

Ist Ihre Pipeline an eine Mehrfachsteckdose oder eine Überspannungsschutzvorrichtung angeschlossen, ist zu überprüfen, ob diese mit dem Netz verbunden und eingeschaltet ist.

Wurde die Pipeline an eine Stromquelle angeschlossen und leuchtet die LED „PWR“, können Sie mit Schritt 3 fortfahren.

Wenn die LED „PWR“ immer noch nicht leuchtet, setzen Sie sich mit Ihrem Händler in Verbindung.

3 Überprüfen Sie die LED „CON“.

Wenn die LED „CON“ innerhalb von dreißig Sekunden nach Anschluß der Pipeline an eine Stromquelle erlischt, ist mit Schritt 4 fortzufahren.

Blinkt die LED „CON“ oder leuchtet sie mehr als 30 Sekunden nach Anschluß der Pipeline an eine Stromquelle, setzen Sie sich mit Ihrem Händler in Verbindung.

4 Drücken Sie die Tastenkombination Strg-L, um den Bildschirm zu aktualisieren.

Wenn kein Profil angezeigt wird, fahren Sie mit Schritt 5 fort.

Erscheint ein Profil, jedoch nicht das „Configure“-Profil, sollten Sie sich den Abschnitt „Es erscheint zwar ein Profil, jedoch nicht das „Configure-Profil““ auf Seite B-9 durchlesen.

5 Überprüfen Sie, daß die Pipeline mit dem seriellen Anschluß Ihres Computers verbunden ist.

Ist dies nicht der Fall, schließen Sie die Pipeline an Ihren Computer an und fahren Sie mit dem nächsten Schritt fort.

Wenn die Pipeline bereits an den Computer angeschlossen ist, fahren Sie mit Schritt 7 fort.

6 Drücken Sie die Tastenkombination Strg-L, um den Bildschirm zu aktualisieren.

Wenn kein Profil angezeigt wird, fahren Sie mit Schritt 7 fort.

Erscheint ein Profil, jedoch nicht das „Configure“-Profil, sollten Sie sich den Abschnitt „Es erscheint zwar ein Profil, jedoch nicht das „Configure-Profil““ auf Seite B-9 durchlesen.

7 Überprüfen Sie die Konfigurationseinstellungen des DFÜ-Programms.

Für die Arbeit mit der Pipeline sollten in Ihrem DFÜ-Programm die folgenden Einstellungen vorgenommen werden:

- VT100
- 9600 Bits/s
- 8 Datenbits
- keine Parität
- 1 Stoppbit
- keine Flußkontrolle
- Direktverbindung

Nehmen Sie, falls erforderlich, die entsprechenden Einstellungen vor, und fahren Sie dann mit dem nächsten Schritt fort.

8 Drücken Sie die Tastenkombination Strg-L, um den Bildschirm zu aktualisieren.

Erscheint auf dem Bildschirm weiterhin kein Profil, sollten Sie sich mit Ihrem Netzwerkadministrator in Verbindung setzen.

Erscheint zwar ein Profil, jedoch nicht das „Configure“-Profil, lesen Sie den nächsten Abschnitt.

Es erscheint zwar ein Profil, jedoch nicht das „Configure-Profil“

Wenn auf Ihrem Bildschirm zwar ein Profil erscheint, es sich dabei aber nicht um das „Configure“-Profil handelt, ist Ihre Pipeline u. U. bereits konfiguriert.

Dieses Problem läßt sich ganz einfach beheben: Drücken Sie die Esc-Taste so lange, bis Sie zum „Main Edit Menu“ zurückgekehrt sind, und wählen Sie dann die Option „Configure“.

Probleme mit ISDN-BRI-Schnittstellen

Probleme bei der Anschlußeinrichtung bzw. Festlegung des Switchtyps

Wenn Sprachrufe nicht ordnungsgemäß empfangen werden, kann dies daran liegen, daß Ihr ISDN-Anschluß in der Vermittlungsstelle nicht richtig eingerichtet wurde. Dies ist um so wahrscheinlicher die Ursache, wenn Ihr ISDN-Anschluß installiert wurde, bevor Sie die für die Pipeline empfohlenen Einrichtungsinformationen kannten.

Wenn Sie keine Sprachrufe empfangen können, solange ein Datenruf existiert, ist Ihr Anschluß möglicherweise mit dem Switchtyp Point-to-Point konfiguriert. Werden beide B-Kanäle für einen Mehrkanal-Datenruf verwendet, ist der Point-to-Point-Switch nicht in der Lage, Sprachrufe an die Pipeline weiterzuleiten.

Sind Sie der Meinung, daß Ihr Problem auf eine falsche Anschlußeinrichtung oder die Verwendung eines falschen Switchs zurückzuführen ist, setzen Sie sich mit Ihrer Telefongesellschaft in Verbindung und gehen Sie mit dieser die zum Beginn dieses Handbuchs beschriebenen Einrichtungsinformationen durch.

Weder das Wählen noch das Beantworten von Rufen funktioniert zuverlässig

Gehen Sie zur Lösung dieses Problems wie folgt vor:

Überprüfen Sie, ob alle Kabel richtig angeschlossen sind.

Der erste und wichtigste Aspekt von ISDN-BRI-Anschlüssen sind die Kabel, die die Pipeline mit dem WAN-Anschluß bzw. den WAN-Endgeräten verbinden. Probleme mit den WAN-Kabeln zeigen sich normalerweise unmittelbar nach der Installation. Wenn Sie sich nicht sicher sind, welche Kabel für Ihre Anwendung benötigt werden, fragen Sie Ihren Händler. In Kapitel 2, „Installation der Pipeline“, werden die allgemeinen Anforderungen an den ISDN-BRI-Anschluß beschrieben, und in Anhang A, „Technische Spezifikationen“, finden Sie eine Aufstellung der Kabelbelegungen.

Probleme beim Bridging bzw. Routing

Die Qualität der Verbindung ist fragwürdig.

Bei der Verwendung von FTP (File Transfer Protocol) wird die Datenübertragungsgeschwindigkeit in Bytes pro Sekunde angegeben. Um diesen Wert in Bits pro Sekunde umzurechnen, müssen Sie ihn mit 8 multiplizieren. Wenn Sie z. B. eine Verbindung mit Köln über einen B-Kanal mit 56-KBit/s herstellen und FTP eine Datenübertragungsgeschwindigkeit von 5,8 KB/s anzeigt, arbeitet die Verbindung mit 5,8 x 8 = 46,8 KBit/s, also mit einer Effektivität von ca. 83 %. Die Effektivität kann von einer Reihe von Faktoren beeinflußt werden, wie z. B. der Belastung des FTP-Servers, der Umlaufverzögerung, dem Gesamtverkehr zwischen den Endpunkten und der Verbindungsqualität.

Die Verbindungsqualität können Sie mit Hilfe des Statusmenüs „WAN Stat“ oder eines Ping-Befehls zwischen denselben Endpunkten überprüfen. Nicht zugestellte Pakete beeinträchtigen die Effektivität der Verbindung ebenso wie die Umlaufverzögerung. Uneinheitliche Umlaufverzögerungswerte weisen auf starken Verkehr hin, was ebenfalls zu einer Beeinträchtigung der Verbindungseffektivität führen kann.

Die Pipeline hängt nach der Beantwortung eines IP-Rufes vorzeitig auf.

Zur Lösung dieses Problems sind die folgenden Schritte auszuführen:

1 Wenn Sie PPP verwenden, überprüfen Sie das von Ihnen eingegebene Kennwort.

2 Stellen Sie sicher, daß für den Parameter „Auth“ „PAP“ oder „CHAP“ festgelegt wurde.

3 Wenn Sie IP-Routing mit PPP verwenden, ist sicherzustellen, daß das rufende Gerät seine IP-Adresse angibt.

Einige rufende Geräte geben zwar ihren Namen, nicht aber ihre IP-Adresse an. Sie können jedoch eine IP-Adresse ableiten, wenn das rufende Gerät in einem lokalen Verbindungsprofil aufgeführt ist. Legen Sie für den Parameter „Recv Auth“ den Wert „PAP“ bzw. „CHAP“ fest, damit die Pipeline den Namen des rufenden Geräts mit dem Wert des Parameters „Station“ in einem Verbindungsprofil vergleicht und auf diese Weise den entsprechenden „LAN Adrs“-Wert ermittelt.

Probleme beim Zugriff auf das entfernte Netzwerk

Wenn Sie im „Configure“-Profil die Tastenkombination Strg-D drücken und im Statusfenster in der rechten oberen Ecke des Bildschirms eine andere Meldung als „LAN Session Up“ erscheint, trennen Sie die Pipeline von der Telefonleitung, schließen Sie sie wieder an, und versuchen Sie erneut, auf das entfernte Netzwerk zuzugreifen. Ist es weiterhin nicht möglich, daß entfernte Netzwerk zu erreichen, kann dies auf eine oder mehrere der folgenden Ursachen zurückzuführen sein:

- Die Pipeline ist nicht ordnungsgemäß installiert.
- Die Pipeline ist nicht ordnungsgemäß konfiguriert.
- Der Telefonanschluß ist nicht aktiviert oder es gibt ein Problem mit dem Telefonnetz.

Überprüfen der Installation

1 Stellen Sie sicher, daß die Pipeline an die Telefonleitung angeschlossen ist.

2 Überprüfen Sie die LED „WAN“ an der Frontblende der Pipeline.

Wenn die LED „WAN“ nicht blinkt, fahren Sie mit den Anweisungen im nächsten Abschnitt, „Konfigurationsprobleme“ auf Seite B-13 fort.

Blinkt die LED „WAN“, kann dies eine der folgenden Ursachen haben:

- Die Pipeline ist nicht mit dem Telefonanschluß verbunden.
- Wenn Sie keine integrierte NT1-Schnittstelle haben, ist Ihre Pipeline u. U. nicht an einen NT1 angeschlossen.
- Ihr Telefonanschluß ist nicht aktiviert.
- Ihr ISDN-Kanal ist vorübergehend nicht verfügbar (Ruhemodus).
- Sie haben einen falschen Wert für „Switch Type“ eingegeben. Überprüfen Sie die Einstellungen im „Configure“-Profil.

3 Stellen Sie sicher, daß Ihre Pipeline mit dem ISDN-Anschluß verbunden ist.

Schließen Sie die Pipeline, falls noch nicht geschehen, an den ISDN-Anschluß an. Wenn Ihre Pipeline keine integrierte NT1-Schnittstelle hat, muß sie mit einem NT verbunden werden. Dieser wiederum ist ordnungsgemäß an den ISDN-Anschluß anzuschließen (siehe dazu das Handbuch zum NT).

Wenn Sie die erforderlichen Anschlüsse hergestellt haben und die LED „WAN“ weiterhin blinkt, fahren Sie mit Schritt 4 fort.

4 Setzen Sie sich mit Ihrem ISDN-Diensteanbieter in Verbindung, um zu überprüfen, ob Ihr Anschluß aktiviert wurde. Ist dies der Fall, fragen Sie nach, ob der Diensteanbieter von Problemen mit dem Telefonnetz weiß.

Ist der Anschluß nicht aktiviert, warten Sie solange, bis dies der Fall ist, und versuchen Sie dann erneut, eine Verbindung mit dem entfernten Netzwerk herzustellen.

Wenn Ihr Diensteanbieter Probleme mit den Leitungen hat, warten Sie eine Weile, und versuchen Sie es dann erneut.

Ist Ihr Anschluß aktiviert und gibt es keine Probleme mit dem Telefonnetz, aber die LED „WAN“ leuchtet immer noch, kann dies an einer falschen Konfiguration liegen. Siehe dazu den nächsten Abschnitt.

Konfigurationsprobleme

Wenn Sie sich sicher sind, daß Ihre Pipeline ordnungsgemäß installiert ist, Ihr Anschluß aktiviert ist und es keine Probleme im Telefonnetz gibt, aber die LED „WAN“ weiterhin blinkt, kann dies auf ein Konfigurationsproblem zurückzuführen sein.

1 Starten Sie Ihr DFÜ-Programm, und drücken Sie die Tastenkombination Strg-L, um den Bildschirm zu aktualisieren.

Im Fenster „Edit“ erscheint das „Configure“-Profil.

2 Überprüfen Sie, ob Ihr „Configure“-Profil gespeichert wurde.

Wenn neben dem Befehl „Save“ ein Sternchen (*) angezeigt wird, haben Sie das „Configure“-Profil geändert, aber nicht gespeichert. Fahren Sie mit Schritt 3 fort.

Wird neben „Save“ kein Sternchen angezeigt, ist mit Schritt 4 fortzufahren.

3 Drücken Sie so lange Strg-N, bis der Befehl „Save“ markiert ist. Drücken Sie dann die Eingabetaste.

Auf diese Weise wird das „Configure“-Profil für die Pipeline gespeichert. Versuchen Sie nun, erneut auf das entfernte Netzwerk zuzugreifen.

Wenn Sie immer noch Probleme haben, fahren Sie mit dem nächsten Schritt fort.

4 Drücken Sie im „Configure“-Profil die Tastenkombination Strg-D, um das entfernte Netzwerk manuell anwählen zu können. Überprüfen Sie dann anhand der Statusfenster 10-100 und 20-100 den Status Ihres ISDN-Anschlusses.

Nähere Informationen zu den Meldungen, die Sie in diesen Fenster sehen können, finden Sie in Anhang C, „Meldungen über Systemereignisse“.

- Erscheint im Feld „Link“ des Statusfensters 10-100 statt eines P, M oder D ein X, ist Ihr ISDN-Anschluß nicht aktiviert oder Sie haben im Parameter „Switch Type“ einen falschen Wert festgelegt.
- Erscheint im Feld „B1“ oder „B2“ ein Sternchen (*) und im Statusfenster „20-100 Sessions“ der Name des entfernten Netzwerks, ist Ihre Pipeline mit dem entfernten Netzwerk verbunden. Fahren Sie mit Schritt 6 fort.

- Erscheint im Feld „B1“ oder „B2“ des Statusfensters 10-100 ein Sternchen (*), das aber wieder verschwindet, ist mindestens eine der folgenden Konfigurationseinstellungen nicht richtig:
  - „Rem Name“: Sie haben u. U. einen falschen Namen für den entfernten Host eingegeben.
  - „Rem Addr“: Sie haben u. U. eine falsche IP-Adresse für den entfernten Host eingegeben.
  - „Send Auth“: Sie haben u. U. das falsche Authentifizierungsprotokoll gewählt.
  - „Send PW“: Sie haben u. U. das Kennwort falsch eingegeben.
  - „My Name“: Der Name, den Sie Ihrer Pipeline zugewiesen haben, stimmt nicht mit dem vom entfernten Host erwarteten Namen überein.
  - „My Addr“: Die für Ihre Pipeline angegebene IP-Adresse ist falsch.
  - Vergleichen Sie die Parameter im „Configure“-Profil mit den Angaben in den Konfigurationstabellen. Stimmen die Werte überein, macht es sich u. U. erforderlich, die Parameter mit dem Netzwerkadministrator abzugleichen.

  Fahren Sie mit Schritt 5 fort.
- Wenn im Feld „B1“ oder „B2“ des Statusfensters 10-100 ein D angezeigt wird, haben Sie u. U. die falsche Telefonnummer für das entfernte Netzwerk angegeben. Fahren Sie mit Schritt 5 fort.

5 Stellen Sie im „Configure“-Profil sicher, daß die Konfigurationsinformationen ordnungsgemäß eingegeben wurden.

Ändern Sie gegebenenfalls die falsch eingegebenen Informationen, und vergessen Sie nicht, das „Configure“-Profil zu speichern.

Wurden die Informationen richtig eingegeben, ist zu überprüfen, daß die Informationen selbst korrekt sind.

- Setzen Sie sich mit Ihrem Netzwerkadministrator in Verbindung, um die Adressen, Namen und die Telefonnummer des entfernten Netzwerks zu bestätigen.

Wenn Sie sich sicher sind, daß die richtigen Informationen richtig eingegeben wurden, und das „Configure“-Profil gespeichert ist, können Sie erneut versuchen, daß entfernte Netzwerk zu erreichen. Haben Sie immer noch Probleme, fahren Sie mit Schritt 6 fort.

6 Wird die Pipeline als Router verwendet, überprüfen Sie, ob die IP-Adresse Ihres Computers ordnungsgemäß konfiguriert wurde.

Hinweise zur Konfiguration der IP-Adresse des Computers entnehmen Sie bitte Ihrem Computer-Handbuch.

Ist es auch jetzt noch nicht möglich, auf das entfernte Netzwerk zuzugreifen, sollten Sie sich mit dem Netzwerkadministrator oder dem Internet-Service-Provider in Verbindung setzen. Bringt dies auch keinen Erfolg, wenden Sie sich bitte an den Ascend Customer Service (Adressen am Anfang dieses Handbuchs).

Meldungen über Systemereignisse

C

Dieser Anhang enthält den folgenden Abschnitt:

Überprüfen der Anzeige im Statusfenster

Systemereignismeldungen zeigen alle Ereignisse an, die in der Pipeline aufgetreten sind, seit sie eingeschaltet wurde. Sie erscheinen im Statusfenster 00-200 (in der rechten oberen Ecke der Bildschirmanzeige).

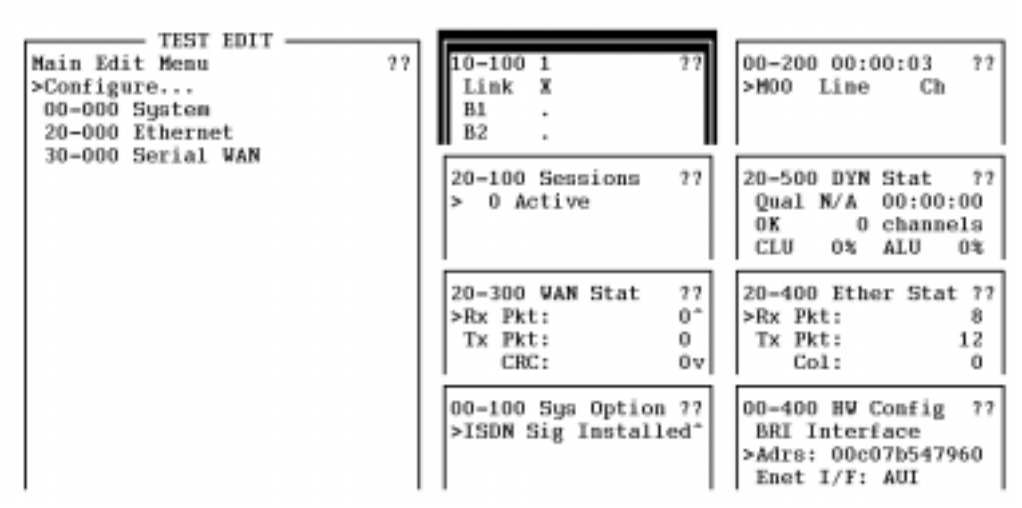


Abbildung C-1: Systemereignismeldungen

Im folgenden finden Sie eine Liste aller möglichen Systemereignismeldungen und ihrer jeweiligen Bedeutung.

Tabelle C-1: Systemereignisse

Ereignismeldung	Bedeutung
Added Bandwidth	Einem aktiven Ruf wurde Bandbreite hinzugefügt.
Assigned To Port	Die Zuordnung eines ankommenden Rufes zur Nummer eines seriellen Host-Anschlusses bzw. zum Ethernet-Modul wurde bestimmt.

Tabelle C-1: Systemereignisse (Fortsetzung)

Ereignismeldung	Bedeutung
Busy	Die Nummer am anderen Ende ist besetzt.
Call Disconnected	Der Ruf wurde unerwartet beendet.
Call Refused	Ein ankommender Ruf konnte nicht mit dem angegebenen seriellen Host-Anschluß verbunden werden, da dieser besetzt oder anderweitig nicht verfügbar war.
Call Terminated	Ein aktiver Ruf wurde normal unterbrochen, jedoch nicht unbedingt durch einen Operatorbefehl.
Ethernet Up	Die Ethernet-Schnittstelle wurde installiert und ist bereit.
Far End Hung Up	Das entfernte Ende hat den Ruf normal beendet.
Incoming Call	Ein ankommender Ruf wurde an der Netzwerk-Schnittstelle beantwortet, ist jedoch bisher weder einem seriellen Host-Anschluß noch dem IP-Router zugewiesen worden.
Incoming Glare	Die Pipeline hat von der Vermittlungsstelle ein ankommendes Gegenbelegungssignal erhalten. Dies kann daran liegen, daß Ihre Telefonleitungen nicht richtig konfiguriert sind.
Incomplete Add	Ein Versuch, einem Invers-Multiplexing-Ruf Kanäle hinzuzufügen, ist mißlungen. Es wurden zwar einige Kanäle hinzugefügt, jedoch weniger als angefordert wurden. Dies kann auch auftreten, wenn beim Initiieren eines Rufes der erste Kanal eine Verbindung herstellt, der angeforderte Basiskanalwert jedoch nicht erreicht wird.

Tabelle C-1: Systemereignisse (Fortsetzung)

Ereignismeldung	Bedeutung
Internal Error	Der Aufbau eines Rufes schlug aufgrund fehlender Systemressourcen, z. B. weil der Hauptspeicher nicht ausreichte, fehl. Bei einem solchen Fehler sollten Sie sich mit dem Technical Assistance Center von Ascend in Verbindung setzen.
LAN Security Error	Eine MPP-, PPP- oder Terminal-Server-Sitzung wurde aufgrund einer Sicherheitsverletzung beendet (z. B. bei Eingabe eines falschen Kennworts).
LAN Session Down	Erscheint vor der Beendigung eines Rufes, wenn eine PPP- oder eine MPP-Sitzung beendet wird.
LAN Session Up	Erscheint nach dem Empfang eines Rufes, wenn eine PPP- oder eine MPP-Sitzung hergestellt wurde.
Network Problem	Der Ruf konnte aufgrund eines Netzwerkproblems nicht ordnungsgemäß beendet werden.
No Chan Other End	Auf der anderen Seite war kein Kanal verfügbar, um einen Ruf aufzubauen.
No Channel Avail	Für den Aufbau des Rufes war kein Kanal verfügbar.
No Connection	Das entfernte Ende hat auf einen ankommenden Ruf nicht geantwortet.
No Phone Number	Im Verbindungsprofil, mit dem Sie versucht haben, einen Ruf aufzubauen, ist keine Telefonnummer angegeben.
No Trunk Available	Alle Leitungen sind außer Betrieb.

Tabelle C-1: Systemereignisse (Fortsetzung)

Ereignismeldung	Bedeutung
Not Enough Chans	Die Anforderung, mehrere Kanäle zu wählen oder die Bandbreite zu erhöhen, konnte nicht ausgeführt werden, da nicht genug Kanäle zur Verfügung standen.
Outgoing Call	Die Pipeline hat einen Ruf gewählt.
Remote Mgmt Denied	Der Versuch, die entfernte Pipeline mittels „Remote Management“ zu betreiben, wurde zurückgewiesen.
Removed Bandwidth	Einem aktiven Ruf wurde Bandbreite abgezogen.
Request Ignored	Die Anforderung zur manuellen Änderung der Bandbreite während eines Rufes wurde abgewiesen.
Trunk Down	Es ist mindestens eine Leitung außer Betrieb.
Trunk Up	Mindestens eine Leitung war außer Betrieb, ist aber wieder betriebsbereit.
Wrong Sys Version	Die Software am anderen Ende ist mit der Systemsoftware der Pipeline nicht kompatibel.

ISDN-Fehlercodes

D

Dieser Anhang enthält die folgenden Abschnitte:

Überprüfen der Statusfenster

Mit Hilfe der ISDN-Fehlercodes können Sie die Ursache von Verbindungsproblemen feststellen. Die Fehlercodes finden Sie im Statusfenster „00-200 System Events“.

Hinweise zur Anzeige des ISDN-Leitungsstatus finden Sie im Chapter 11, “Systemadministration,”.

Liste der Fehlercodes

Die in dieser Tabelle aufgelisteten Fehlercodes gelten nicht für 1TR6-Netze (WANs) in Deutschland. Die für diese Netze gültigen Fehlercodes entnehmen Sie bitte dem Abschnitt „ 1TR6-ISDN-Fehlercodes“ auf Seite D-7.

Hinweis: Die Fehlercodes können, je nach Konfiguration der jeweiligen Vermittlungsstelle, unterschiedlich implementiert sein. Setzen Sie sich mit Ihrem ISDN-Diensteanbieter in Verbindung, wenn Sie Fragen zu den von Ihrer Vermittlungsstelle unterstützten Fehlercodes haben.

Tabelle D-1: ISDN-Fehlercodes

Code	Ursache
0	noch keinen gültigen Fehlercode empfangen
1	nicht zugewiesene Nummer
2	keine Route zum angegebenen Transitnetz (WAN)
3	keine Route zum Ziel
4	speziellen Informationston senden
5	falsch gewähltes Trunk-Präfix
6	Kanal nicht akzeptabel
7	Ruf zuerkannt und über einen aufgebauten Kanal geliefert

Tabelle D-1: ISDN-Fehlercodes (Fortsetzung)

Code	Ursache
8	Präfix 0 gewählt, aber nicht gültig
9	Präfix 1 gewählt, aber nicht gültig
10	Präfix 1 gewählt, aber nicht erforderlich
11	mehr Ziffern empfangen als erlaubt, Ruf wird fortgesetzt
16	normale Rufbeendigung
17	Benutzer besetzt
18	kein Benutzer antwortet
19	keine Antwort vom Benutzer (Benutzer wurde alarmiert)
21	Ruf zurückgewiesen
22	Nummer geändert
23	R-Gespräch zurückgewiesen
24	Ruf unterbrochen
25	Ruf wiederaufgenommen
26	nicht ausgewählter Benutzerabbruch
27	Ziel defekt
28	ungültiges Nummernformat (Nummer unvollständig)
29	Leistungsmerkmal abgewiesen
30	Antwort auf Statusabfrage (STATUS ENQUIRY)
31	normal, keine weiteren Angaben

Tabelle D-1: ISDN-Fehlercodes (Fortsetzung)

Code	Ursache
33	Schaltung defekt
34	kein(e) Schaltung/Kanal verfügbar
35	Ziel unerreichbar
37	Dienst beeinträchtigt
38	Netz (WAN) außer Betrieb
39	Transitverzögerungsbereich konnte nicht erreicht werden
40	Durchsatzbereich konnte nicht erreicht werden
41	temporärer Ausfall
42	Vermittlungsstelle überlastet
43	Zugangsinformationen ignoriert
44	angeforderter Schaltungskanal nicht verfügbar
45	Zwangstrennung
46	Vorrangruf blockiert
47	Ressource nicht verfügbar, keine weiteren Angaben
49	Dienstqualität nicht verfügbar
50	angefordertes Leistungsmerkmal nicht angemeldet
51	R-Gespräch nicht erlaubt
52	abgehende Rufe gesperrt
53	abgehende Rufe innerhalb CUG gesperrt

Tabelle D-1: ISDN-Fehlercodes (Fortsetzung)

Code	Ursache
54	ankommende Rufe gesperrt
55	ankommende Rufe innerhalb CUG gesperrt
56	Anklopfen nicht angemeldet
57	Trägerleistungsmerkmal nicht genehmigt
58	Trägerleistungsmerkmal gegenwärtig nicht verfügbar
63	Dienst bzw. Option nicht verfügbar, keine weiteren Angaben
65	Übermittlungsdienst nicht implementiert
66	Kanaltyp nicht implementiert
67	ausgewähltes Transitnetz nicht implementiert
68	Meldung nicht implementiert
69	angefordertes Leistungsmerkmal nicht implementiert
70	nur begrenzte digitale Informationsträgerfunktion verfügbar
79	Dienst bzw. Option nicht implementiert, keine weiteren Angaben
81	ungültiger Wert für die Rufkennung
82	angegebener Kanal existiert nicht
83	ein unterbrochener Ruf existiert, nicht aber diese Rufkennung
84	Rufkennung wird benutzt

Tabelle D-1: ISDN-Fehlercodes (Fortsetzung)

Code	Ursache
85	kein Ruf unterbrochen
86	Ruf mit angeforderter Rufkennung wurde beendet
87	gerufener Benutzer nicht Teilnehmer des CUG-Netzes
88	inkompatibles Ziel
89	Kurzadresseneintrag existiert nicht
90	Zieladresse fehlt und direkter Ruf nicht angemeldet
91	ausgewähltes Transitnetz ungültig (Verwendung national)
92	ungültiger Leistungsmerkmalparameter
93	obligatorisches Informationselement fehlt
95	ungültige Meldung, keine weiteren Angaben
96	obligatorisches Informationselement fehlt
97	Meldungstyp existiert nicht oder ist nicht implementiert
98	Meldung mit dem Rufstatus oder dem Meldungstyp nicht kompatibel, nicht existent oder nicht implementiert
99	Informationselement nicht existent oder nicht implementiert
100	ungültiger Inhalt des Informationselements
101	Meldung mit dem Rufstatus nicht kompatibel
102	Wiederherstellungs-Timeout abgelaufen

Tabelle D-1: ISDN-Fehlercodes (Fortsetzung)

Code	Ursache
103	Parameter existiert nicht oder ist nicht implementiert, weitergeleitet
111	Protokollfehler, keine weiteren Angaben
127	Querruf, keine weiteren Angaben

1TR6-ISDN-Fehlercodes

Alle Produkte, die BRI unterstützen, können optional auch 1TR6-Vermittlungsstellen unterstützen. Die ISDN-Fehlercodes für 1TR6 unterscheiden sich von den Codes für Vermittlungsstellen vom Typ AT&T, NI-1, NTI und von anderen Vermittlungsstellen. In Table D-2 finden Sie die ISDN-Fehlercodes für 1TR6-Vermittlungsstellen.

Tabelle D-2: 1TR6-ISDN-Fehlercodes

Code	Ursache	Erklärung
1	ungültige Rufkennung	ungültiger CR-Wert
3	Trägerdienst nicht implementiert	Dienst ist in der A-Vermittlung oder an anderer Stelle des Netzes nicht verfügbar bzw. der Dienst wurde nicht beantragt
7	Rufkennung existiert nicht	unbekannte Rufkennung

Tabelle D-2: 1TR6-ISDN-Fehlercodes (Fortsetzung)

Code	Ursache	Erklärung
8	Rufkennung in Benutzung	Rufkennung ist bereits einem unterbrochenen Ruf zugewiesen
10	kein Kanal verfügbar	für die Teilnehmeranschlußleitung steht kein nutzbarer Kanal zur Verfügung (nur von lokaler Bedeutung)
16	angefordertes Leistungsmerkmal nicht implementiert	der angegebene FAC-Code ist in der A-Vermittlung oder an einer anderen Stelle im Netz nicht bekannt
17	Anfrage-Leistungsmerkmal nicht angemeldet	Anfrage-Leistungsmerkmal abgewiesen, da A- oder B-Teilnehmer nicht über die entsprechenden Rechte verfügt
32	abgehende Rufe gesperrt	abgehende Rufe aufgrund der installierten Zugriffsbeschränkungen nicht möglich

Tabelle D-2: 1TR6-ISDN-Fehlercodes (Fortsetzung)

Code	Ursache	Erklärung
33	Benutzeranschluß besetzt	Wenn die Summe aus der Anzahl der freien B-Kanäle und der Anzahl der Rufvorgänge ohne definierten B-Kanal gleich vier ist, werden alle ankommenden Rufe im Netz gelöscht. Die rufende Seite erhält ein DISC und als Ursache „user access busy“ (= erste Besetztinstanz). Außerdem ertönt das Besetztzeichen.
34	CUG-Vergleich negativ	Verbindung aufgrund eines negativen CUG-Vergleichs nicht möglich
35	CUG nicht existent	CUG existiert nicht
37	semipermanente Verbindung nicht gestattet	Verbindung ist nicht möglich, z. B. aufgrund einer negativen RFNR-Überprüfung
48 - 50	nicht benutzt	

Tabelle D-2: 1TR6-ISDN-Fehlercodes (Fortsetzung)

Code	Ursache	Erklärung
53	Ziel nicht erreichbar	Verbindung im Netz kann wegen falscher Zieladresse, falscher Dienste oder falscher Leistungsmerkmale nicht aufgebaut werden
56	geänderte Nummer	Nummer des B-Teilnehmers hat sich geändert
57	außer Betrieb	entferntes Endgerät nicht bereit
58	kein Benutzer antwortet	das ankommende SETUP ist von keinem Endgerät beantwortet worden oder der Ruf wurde wegen angenommener Abwesenheit abgebrochen (Ruf-Timeout T3AA abgelaufen)
59	Benutzer besetzt	B-Teilnehmeranschluß ist besetzt
61	ankommende Rufe gesperrt	der B-Teilnehmer hat den Zugang für ankommende Rufe beschränkt oder der angeforderte Dienst wird vom B-Teilnehmer nicht unterstützt

Tabelle D-2: 1TR6-ISDN-Fehlercodes (Fortsetzung)

Code	Ursache	Erklärung
62	Ruf abgewiesen	für A-Teilnehmer: Verbindungsanforderung aktiv vom B-Teilnehmer abgewiesen (auf ein ankommendes SETUP wurde ein DISC gesendet) für ein Endgerät in der Phase, in der ein ankommender Ruf aufgebaut wird: Ruf ist bereits von einem anderen TE am Bus angenommen worden
89	Netz verstopft	Nadelöhr im Netz, z. B. alle Verbindungsleitungen besetzt, keine Konferenz freigegeben
90	vom entfernten Benutzer initiiert	vom entfernten Benutzer bzw. der entfernten Vermittlung abgewiesen oder beendet

Tabelle D-2: 1TR6-ISDN-Fehlercodes (Fortsetzung)

Code	Ursache	Erklärung
112	lokaler Prozedurfehler	in REL: Ruf aufgrund von lokalen Fehlern beendet (z. B. ungültige Meldungen oder Parameter, abgelaufenes Timeout usw.) in SUS REJ: Verbindung darf nicht unterbrochen werden, da bereits anderes Leistungsmerkmal aktiv ist in RES REJ: kein unterbrochener Ruf verfügbar in FAC REJ: es kann kein weiteres Leistungsmerkmal angefordert werden, da bereits ein Leistungsmerkmal verarbeitet wird, bzw. das angeforderte Leistungsmerkmal kann im gegenwärtigen Rufstatus nicht angefordert werden
113	entfernter Prozedurfehler	Ruf aufgrund eines Fehlers auf der entfernten Seite abgebrochen

Tabelle D-2: 1TR6-ISDN-Fehlercodes (Fortsetzung)

Code	Ursache	Erklärung
114	Ruf durch entfernten Benutzer unterbrochen	Ruf wurde vom entfernten Benutzer auf Halten geschaltet oder unterbrochen
115	Ruf vom entfernten Benutzer wiederaufgenommen	Ruf ist am entfernten Ende nicht mehr auf Halten geschaltet, unterbrochen oder im Konferenzstatus
127	Benutzerinfo lokal abgewiesen	die Meldung USER INFO wurde lokal abgewiesen; diese Ursache wird in der Meldung CON angegeben

Aktualisieren der Systemsoftware

E

Dieser Anhang enthält die folgenden Abschnitte:

Voraussetzugen für die Aktualisierung der Systemsoftware

Die Ascend-Systemsoftware wird ständig weiterentwickelt, um neue Funktionen zu integrieren und die Leistungsfähigkeit zu erhöhen. Die Pipeline ist so konstruiert, daß Sie die Systemsoftware aktualisieren und damit diese neuen Funktionen nutzen können, ohne das Gerät zum Werk zurücksenden zu müssen.

Zur Aktualisierung der Systemsoftware wird folgendes benötigt:

- Die neue Systemsoftware. Diese erhalten Sie von Ihrem Händler oder über FTP.ASCEND.COM (anonyme Anmeldung und E-Mail-Adresse als Kennwort).
- Eine serielle Verbindung zwischen einem PC und der Pipeline für den Zugriff auf die Konfigurationssoftware mit Hilfe Ihres DFÜ-Programms.

Hinweis: Diese Prozedur ist *nicht* für Windows-Versionen von DFÜ-Programmen geeignet. Wenn Sie mit einem DFÜ-Programm für den Macintosh arbeiten, muß die Option „MacBinary“ deaktiviert werden.

Die Aktualisierungsprozedur

Die Aktualisierung der Systemsoftware erfolgt, abhängig vom jeweils aktiven Sicherheitsprofil, in vier oder fünf Stufen. Die Prozedur umfaßt die folgenden Hauptschritte:

1 Aktivieren eines Sicherheitsprofils, das die Feldaktualisierung erlaubt (falls erforderlich)

2 Sichern der konfigurierten Profile auf der Festplatte des Computers

3 Herunterladen der Systemsoftware

4 Wiederherstellen der Pipeline-Konfiguration

Diese Aufgaben werden in diesem Anhang genauer beschrieben. Bevor Sie weitermachen, sollten Sie zunächst überprüfen, welche Version der Systemsoftware gegenwärtig in Ihrer Pipeline installiert ist und welches Sicherheitsprofil aktiviert wurde.

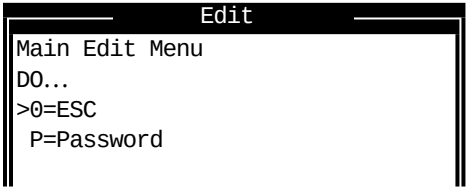
Die gegenwärtige Software-Version können Sie dem Statusfenster „Sys Option“ entnehmen. Weitere Informationen dazu finden Sie im Appendix C, “Meldungen über Systemereignisse”.

Aktivieren eines Sicherheitsprofils

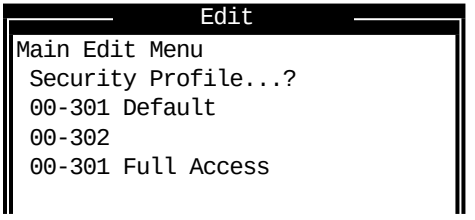
Wenn der Parameter „Field Service“ im gegenwärtig aktivierten Sicherheitsprofil den Wert „No“ hat, müssen Sie zur Aktualisierung der Systemsoftware zunächst ein Sicherheitsprofil aktivieren, bei dem für „Field Service“ der Wert „Yes“ festgelegt wurde.

Zum Aktivieren des Sicherheitsprofils mit „Field Service=Yes“ ist wie folgt vorzugehen:

1 Drücken Sie die Tastenkombination Strg-D, um das DO-Menü zu öffnen. Drücken Sie dann die Taste P (oder markieren Sie „P=Password“).

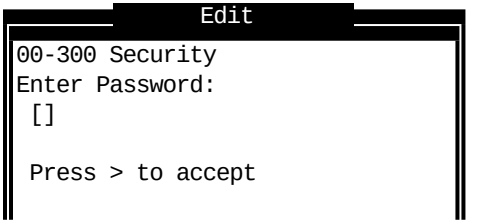


2 Markieren Sie in der sich daraufhin öffnenden Liste der Sicherheitsprofile das gewünschte Sicherheitsprofil. Im „Full-Access“-Profil ist „Field Service“ standardmäßig aktiviert.

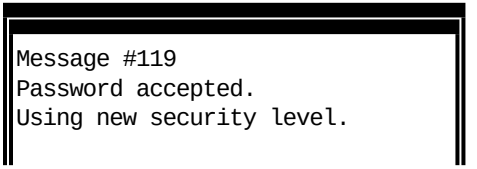


Sie werden dann aufgefordert, daß Kennwort für das Profil einzugeben.

3 Geben Sie das dem Profil zugewiesene Kennwort ein, und drücken Sie dann die Eingabetaste, um es zu akzeptieren.



Wenn Sie das richtige Kennwort eingegeben haben, erscheint eine Meldung, die besagt, daß das Kennwort akzeptiert wurde und die Pipeline jetzt mit einer neuen Sicherheitsstufe arbeitet.



Ist das von Ihnen eingegebene Kennwort nicht richtig, werden Sie erneut aufgefordert, das richtige Kennwort einzugeben.

Sichern der Pipeline-Konfiguration

Bevor Sie die Software in der Pipeline überschreiben, sollten Sie Ihre Konfiguration auf der Festplatte speichern.

Hinweis: Beim Speichern der Pipeline-Konfiguration werden die Konfigurationsdaten in eine Textdatei auf der Festplatte des Host-Computers geschrieben, der mit dem „Terminal“-Anschluß der Pipeline verbunden ist. *Kennwörter werden nicht mit gespeichert!* Wenn Sie eine Konfiguration anhand einer gespeicherten Datei wiederherstellen, werden die Parameter „Send PW“, „Recv PW“ sowie die Kennwörter für die Sicherheitsprofile und die im Ethernet-Profil (Menü „Mod Config“) festgelegten Kennwörter alle auf das „Null-Kennwort“ gesetzt (für den Zugang reicht dann das Drücken der Eingabetaste). Wir empfehlen daher dringend, sich diese Kennwörter zu notieren und sicher aufzubewahren, falls sie wiederhergestellt werden müssen.

Bevor Sie beginnen, sollten Sie sicherstellen, daß Ihre Terminal-Emulation das Speichern der am seriellen Anschluß empfangenen ASCII-Zeichen auf der Festplatte erlaubt. Außerdem ist zu kontrollieren, daß die Datenübertragungsgeschwindigkeit des Terminal-Emulationsprogramms auf maximal 9600 Bit/s eingestellt ist, und daß für den Parameter „Term Rate“ im Systemprofil (Menü „Sys Config“) ebenfalls der Wert „9600“ festgelegt wurde. Bei höheren Geschwindigkeiten können Fehler beim Speichern der Zeichen auftreten.

Sie können den Sicherungsvorgang jederzeit abbrechen. Drücken Sie dazu die Tastenkombination Strg-C.

Mit den folgenden Schritten können Sie die Pipeline-Konfiguration (mit Ausnahme der Kennwörter) auf der Festplatte speichern:

1 Öffnen Sie das Menü „Sys Diag“.

2 Wählen Sie den Befehl „Save Config“, und drücken Sie die Eingabetaste.
Es erscheint die folgende Meldung:

```
Ready to download - type any key to start...
```

3 Aktivieren Sie die Zeichenspeicherungsfunktion Ihres DFÜ-Programms, und geben Sie einen Dateinamen für die gespeicherten Profile an.
Wenn Sie Fragen zur Aktivierung der Zeichenspeicherungsfunktion haben, schlagen Sie in der Dokumentation zu Ihrem DFÜ-Programm nach.

4 Drücken Sie eine beliebige Taste, um das Speichern der konfigurierten Profile zu starten.
Auf dem Bildschirm erscheinen während des Speicherns auf die Festplatte die verschiedensten Konfigurationsinformationen. Nach Abschluß des Speichervorgangs erscheint eine entsprechende Meldung.

5 Deaktivieren Sie die Zeichenspeicherfunktion Ihres DFÜ-Programms.

6 Drucken Sie ein Exemplar der konfigurierten Profile aus, um gegebenenfalls später darauf zurückgreifen zu können.

Hinweis: Bei der Betrachtung der gespeicherten Pipeline-Datendatei werden Sie feststellen, daß einige der Zeilen mit *START=* und andere mit *END=* beginnen. Diese START/STOP-Zeilen und der dazwischenliegende Datenblock sind ein Profil. Wenn ein Parameter in einem Profil auf seinen Standardwert gesetzt wird, erscheint dieser nicht im Profil. Wenn also für alle Parameter in

einem Profil der Standardwert festgelegt wurde, ist der entsprechende START/ STOP-Block leer.

Laden der Systemsoftware

Hinweis: Beim Laden der Systemsoftware werden alle existierenden Profile überschrieben. Sie sollten daher vor dem Aktualisieren der Systemsoftware alle aktuellen Profile auf Ihrer Festplatte speichern, um zu vermeiden, daß Sie sämtliche Profile neu konfigurieren müssen.

Versetzen Sie die Pipeline in den Boot-Modus. Gehen Sie dazu wie folgt vor:

1 Drücken Sie in jedem beliebigen Menü in der Pipeline-Software nacheinander so schnell wie möglich die folgenden Tasten:

Esc [Esc -

Benutzen Sie dazu eine US-Tastatur, oder benutzen Sie bei einer deutschen Tastatur die Tastenkombination STRG+F1 zum Umschalten von der deutschen Tastaturbelegung zur amerikanischen. Zurück wechseln Sie mit STRG-F2.

„Esc“ ist die Escape-Taste, „[“ ist die linke eckige Klammer und „-“ ist die Minustaste. Drücken Sie die Tasten genau in der angegebenen Reihenfolge, eine nach der anderen und so schnell wie möglich. Wenn auf Ihrem Bildschirm nicht die Xmodem-Steuerzeichen

CKCKCKCK

erscheinen, liegt das am ehesten daran, daß Sie die Tasten nicht schnell genug hintereinander gedrückt haben. Versuchen Sie es in diesem Fall noch einmal. Die meisten Leute verwenden dazu beide Hände und lassen einen Finger auf der Esc-Taste liegen.

2 Sobald die Xmodem-Steuerzeichen

CKCKCKCK

erscheinen, können Sie beginnen, die Systemdatei mit Hilfe des Dateitransferprotokolls Xmodem auf Ihre Pipeline herunterzuladen. Dies dauert im Normalfall zwischen 5 und 15 Minuten.

Hinweis: Die auf dem Bildschirm angezeigte Zeit ist keine Echtzeitangabe. Wenn Ihr DFÜ-Programm des öfteren meldet, daß ein fehlerhaftes Datenpaket gesendet wurde, ist dies kein Grund zur Beunruhigung, sondern ganz normal.

Nach Abschluß des Ladevorgangs setzt sich die Pipeline selbst zurück. Wenn der Selbsttests abgeschlossen wurde, erscheint im „Edit“-Fenster das „Configure“-Profil, wobei alle Parameter ihren Standardwert haben.

Sie können nun Ihre konfigurierten Profile wiederherstellen. Fahren Sie dazu mit den Anweisungen im nächsten Abschnitt fort.

Wiederherstellen der Pipeline-Konfiguration

Nachdem Sie Ihre Systemsoftware aktualisiert haben, können Sie Ihre konfigurierten Profile wiederherstellen.

Hinweis: Wenn Sie den Befehl „Restore Cfg“ verwenden, erscheinen zuweilen am Ende der gespeicherten Konfigurationsdatei zusätzliche Daten. Die konfigurierte Datei muß mit dem Wort START beginnen und mit den Wörtern END DOWNLOAD aufhören. Vor der Wiederherstellung der Daten empfiehlt es sich zu überprüfen, ob Ihre Textdatei dieses Format aufweist.

Hinweis: Wenn die aktualisierte Systemsoftware neue Parameter beinhaltet, macht es sich u. U. erforderlich, neben den neuen Parametern auch einige der bereits zuvor vorhandenen Parameter neu zu konfigurieren.

Vor dem Beginn der Wiederherstellungsprozedur sollten Sie sich vergewissern, daß Ihr Terminalemulationsprogramm über eine Autotype-Funktion (bzw. eine ASCII-Dateien-Upload-Funktion) verfügt. Mit Hilfe der Autotype-Funktion kann Ihr Emulationsprogramm Textdateien über den seriellen Anschluß senden. Außerdem ist sicherzustellen, daß die Datenübertragungsgeschwindigkeit des Terminalemulationsprogramms auf maximal 9600 Bit/s eingestellt ist. Der Parameter „Term Rate“ im Systemprofil (Menü „Sys Config“) muß ebenfalls auf 9600 eingestellt sein. Höhere Geschwindigkeiten können zu Übertragungsfehlern führen.

Der Befehl „Restore Cfg“ kann verwendet werden, um eine vollständige Konfiguration, die Sie zuvor mit dem Befehl „Save Cfg“ gespeichert haben, wiederherzustellen oder um spezifischere Konfigurationsinformationen, die Sie von Ascend erhalten haben (z. B. einen einzelnen, in einer speziellen Konfigurationsdatei gespeicherten Filter), hochzuladen. Zum Laden von Konfigurationsinformationen von der Festplatte müssen Sie zunächst das

Backup-Gerät an den „Control“-Anschluß der Pipeline anschließen. Gehen Sie dann wie folgt vor:

1 Markieren Sie im Menü „Sys Diag“ die Option „Restore Cfg“, und drücken Sie die Eingabetaste.

Es erscheint die folgende Meldung:

```
Waiting for upload data...
```

2 Senden Sie mit Hilfe der Funktion „ASCII-Datei senden“ Ihres DFÜ-Programms die Konfigurationsdatei an die Pipeline.

Sollten Sie Fragen zum Senden von ASCII-Dateien haben, finden Sie die entsprechenden Informationen in der Dokumentation zu Ihrem DFÜ-Programm. Nach Abschluß der Wiederherstellung erscheint die folgende Meldung:

```
Restore complete - type any key to return to menu
```

3 Drücken Sie eine beliebige Taste, um zum Konfigurationsmenü zurückzukehren.

Wenn Sie eine vollständige Konfiguration wiederhergestellt haben, sind die Kennwörter in Ihren Sicherheitsprofilen nicht mehr vorhanden. Sollen Sie erneut festgelegt werden, ist wie folgt vorzugehen:

1 Drücken Sie die Tastenkombination Strg-D. Es erscheint das DO-Menü. Markieren Sie die Option „Password“, und wählen Sie das Profil „Full Access“.

2 Drücken Sie die Eingabetaste („Null-Kennwort“), sobald Sie aufgefordert werden, ein Kennwort einzugeben.

Nachdem Sie Ihre Zugriffsrechte wiederhergestellt haben, indem Sie festgelegt haben, daß das „Null-Kennwort“ verwendet werden soll, empfehlen wir, sofort die Verbindungsprofile, Sicherheitsprofile und das Ethernet-Profil (Menü „Mod Config“) zu öffnen und die vorherigen Einstellungen für die Kennwörter wiederherzustellen.

Sollen die Sicherheitsstufen für die aktualisierte Pipeline wiederhergestellt werden, ist das entsprechende Sicherheitsprofil erneut zu aktivieren. Verwenden Sie dazu die im Abschnitt „Aktivieren eines Sicherheitsprofils“ auf Seite E-3 beschriebene Prozedur, und wählen Sie das entsprechende Sicherheitsprofil aus.

Ascend-Glossar

F

Dieses Glossar enthält Erläuterungen von Begriffen, die für die gesamte Ascend-Produktfamilie, also sowohl für Pipeline- als auch für MAX-Einheiten, gelten.
10BaseT – IEEE-Standard (802.3) für den Betrieb von 10-MBit/s-Ethernet-Netzwerken mit Twisted-Pair-Kabeln und Hubs.

analoge Daten – Daten, die jeden Wert innerhalb eines bestimmten Bereichs haben und sich ständig ändern können; Beispiele für analoge Daten sind die durch Zeiger angezeigte Uhrzeit oder die mit Hilfe eines Flüssigkeitsthermometers angezeigte Temperatur.

analoges Signal – Signaltyp, der Daten verschlüsselt, die über ein Kabel oder durch die Luft gesendet werden, und der im allgemeinen durch eine oszillierende Welle dargestellt wird. Ein analoges Signal kann jeden Wert innerhalb eines bestimmten Bereichs annehmen. Die Änderung von Werten erfolgt stufenlos.

Analoge Signale können analoge oder digitale Daten übertragen. So kann z. B. eine Radiostation analoge Musikdaten mit Hilfe von analogen Signalen übertragen, oder ein Modem kann analoge Signale für die Übertragung von digitalen Daten nutzen.
ARP – *Address Resolution Protocol*. Dieser Teil des TCP/IP-Protokolls dient zur Kennzeichnung der PCs in einem Ethernet-LAN, indem es der physikalischen Adresse (Ethernet-Adresse) des PC, auf dem es läuft, eine IP-Adresse zuweist.

asynchrone Übertragung – Modus, bei dem sowohl der sendende als auch der empfangende serielle Host weiß, wo ein Zeichen beginnt und endet, da jedes Byte am Anfang bzw. am Ende mit zusätzlichen Bits, dem *Startbit* und dem *Stopbit*, versehen wird. Das Startbit zeigt den Anfang eines neuen Zeichens an und ist immer 0 (Null). Das Stopbit markiert das Ende des Zeichens. Es erscheint nach dem Paritätsbit, falls ein solches verwendet wird.

AUI – *Autonomous Unit Interface* oder *Attachment Unit Interface*. Dies ist die Bezeichnung der 15poligen D-Buchse und der Kabel, die Ein- und Mehrkanalkomponenten in einem Ethernet-Transceiver miteinander verbinden.

Backbone – Der Teil des Kommunikationsnetzes, über den der Großteil des Verkehrs läuft. Ermöglicht die Verbindung von Subnetzen in unternehmensweiten Netzwerken.

Backbone-Router – Router, die für den Aufbau von Backbone-Netzwerken mittels Mietleitungen bestimmt sind. Sie besitzen im Normalfall keine eingebauten digitalen Einwahl-WAN-Schnittstellen. Zu den Herstellern von Backbone-Routern gehören die Firmen Cisco, Wellfleet, 3Com, CrossCom u. a.

Bit – Zusammenziehung aus *BInary digiT*. Kleinste Informationseinheit, die von einem Computer verarbeitet werden kann; kann einen von zwei Werten annehmen (im Normalfall dargestellt durch „1“ und „0“).

B-Kanal – 64-KBit/s-Kanal für die Übertragung von Benutzerdaten.

Bridge (Brücke) – Gerät oder Vorrichtung zur Verbindung zweier Netzwerksegmente für die Übertragung von Daten, Sprache oder Video auf der Grundlage der Zielangabe im Paketheader. Ascend-Einheiten sind „intelligente“ Bridges, denn sie leiten alle Pakete zum nächsten Netzwerksegment (der ISDN-Leitung) weiter und erstellen eine Tabelle, mit deren Hilfe die lokalen und entfernten Zieladressen zugeordnet werden können. Wenn sie die Adressen auf beiden Seiten des Netzwerks „gelernt“ hat, leitet die Brücke nur die Pakete für das entfernte Netzwerk weiter (im Gegensatz zum Router).

CDR – *Call Detail Reporting* (Rufdatenerfassung). Leistungsmerkmal, bei dem in einer Datenbank die folgenden Informationen zu jedem einzelnen Ruf aufgezeichnet werden: Datum, Uhrzeit, Dauer, gerufene Nummer, rufende Nummer, Rufrichtung, Diensttyp und die jeweilige Invers-Multiplex-Sitzung und der entsprechende Anschluß. Da der Netzwerkträger die Bandbreitennutzung auf der Basis der tatsächlich verwendeten Bandbreite und jede Verbindung in einem Invers-Multiplex-Ruf einzeln berechnet, können Sie sich mit CDR einen Überblick über die Bandbreitennutzung und die Kosten jeder einzelnen Invers-Multiplex-Sitzung verschaffen und die entsprechenden Schritte einleiten.

Sie können die Angaben ändern, um so die verschiedensten Berichte anzufertigen. So können z. B. Berichte auf der Basis der Kosten pro Ruf, der Kosten für inverse Multiplex-WAN-Sitzungen, der Kosten pro Anwendung, der Muster für die Bandbreitennutzung über einen bestimmten Zeitraum usw. angefertigt werden. Diese Informationen helfen Ihnen dabei, Ihre

Bandbreitennutzungsmuster besser einschätzen zu können und gegebenenfalls Änderungen des Verhältnisses zwischen gewählten Verbindungen und Festverbindungen zwischen Netzstandorten vorzunehmen.

CHAP – *Challenge Handshake Authentication Protocol*. Dieses Sicherheitsprotokoll ermöglicht den Zugang zwischen Datenübertragungssystemen vor und während der Datenübertragung. Zur Überprüfung der Zugriffsrechte des Benutzers verwendet CHAP sogenannte „Challenges“.

Codec – *COder/DECoder.* Gerät, das analoge Daten für die Übertragung über ein digitales Medium in ein digitales Signal umwandelt.

CPE – *Customer Premises Equipment*. Siehe „Teilnehmereinrichtung“.

CSU – *Channel Service Unit*. Gerät zur Verbindung einer digitalen Telefonleitung vom Telefonnetz mit der Netzzugangseinrichtung am Teilnehmerstandort. Eine CSU kann auch in die Netzwerkschnittstelle der Netzzugangseinrichtung integriert sein.

Datendienst – Über eine WAN-Leitung zur Verfügung gestellter Dienst, der durch seine Bandbreite charakterisiert wird. Ein Datendienst kann entweder Daten oder digitalisierte Sprache übertragen.

DBA – *Dynamic Bandwidth Allocation* (dynamische Bandbreitenzuweisung). Hinzufügen oder Abziehen von Bandbreite zu bzw. von einer Wählverbindung in Echtzeit, ohne dabei die Verbindung zu beenden. Die dynamische Bandbreitenzuweisung wird von MPP und AIM unterstützt. Dazu sind eine Reihe von Parameterwerten festzulegen.

Die Berechnung der mittleren Leitungsnutzung (Average Line Utilization, ALU) durch Ascend-Einheiten erfolgt auf der Grundlage des im Parameter „Sec History“ angegebenen historischen Zeitabschnitts. Dieser Wert wird dann mit dem im Parameter „Target Util“ angegebenen Wert verglichen. Wenn der ALU-Wert den im Parameter „Target Util“ festgelegten Grenzwert länger überschreitet, als im Parameter „Add Pers“ angegeben, versucht die Pipeline, die im Parameter „Inc Ch Count“ angegebene Zahl der Kanäle hinzuzufügen. Fällt der ALU-Wert länger als im Parameter „Sub Pers“ angegeben unter den in „Target Util“ festgelegten Grenzwert, versucht die Pipeline, die im Parameter „Dec Ch Count“ angegebene Zahl der Kanäle abzuziehen.

Wenn Sie eine Schaltung zwischen zwei Standorten benötigen, die 24 Stunden am Tag verfügbar ist, ist eine Festverbindung kostengünstiger als eine Wählleitung (gewählte Leitung). Benötigen Sie die Schaltung jedoch nur hin und

wieder, oder wird sie zu bestimmten Zeiten nicht voll ausgenutzt, ist es oft sinnvoller, eine kleinere Menge festgeschalteter Bandbreite zu mieten und diese dann mit zusätzlicher vermittelter Bandbreite zu ergänzen, wenn die Verkehrsbelastung dies erfordert.

So brauchen bestimmte Verbindungen nur dann aufgebaut zu werden, wenn Daten übertragen werden müssen. Bei geringem Verkehr reicht eine Einzelschaltung. Wenn das Verkehrsaufkommen jedoch die Kapazität der Schaltung übersteigt (wie z. B. bei der Übertragung großer Dateien), fügt die dynamische Bandbreitenzuweisung automatisch gewählte Kanäle hinzu. Wird das Verkehrsaufkommen wieder geringer, werden die zusätzlichen Kanäle automatisch wieder der Verbindung entzogen. Auf diese Weise werden die Bandbreiten- und Verbindungskosten reduziert, da Sie nur dann für Bandbreite zahlen, wenn Sie sie brauchen.

DCE – *Data Communications Equipment* (Datenübertragungseinrichtung). In der RS-232-Spezifikation beschriebene Einrichtung, mit der die DTE (Data Terminal Equipment, Datenendeinrichtung) verbunden ist, um z. B. den Zugang zu den Netzwerkeinrichtungen zu ermöglichen. Die DCE wandelt das Format der von der DTE gesendeten Daten in ein für den Übertragungskanal geeignetes Signal um. Die Bezeichnung DCE wird für Geräte wie Netzzugangseinrichtungen verwendet, während DTE häufig für Anwendungsgeräte wie z. B. Videokonferenzterminals verwendet wird.

digitale Daten – Daten, die nur eine begrenzte Anzahl von getrennten Werten haben können. Beispiele für digitale Daten sind die Angabe der Uhrzeit durch eine Digitaluhr oder die Angabe der Temperatur durch ein digitales Thermometer. Die digitalen Werte ändern sich nicht kontinuierlich, sondern bleiben auf einem bestimmten Wert und wechseln dann zu einem anderen bestimmten Wert.

digitales Modem – Internes Gerät in der MAX-Einheit, das diese in die Lage versetzt, über eine digitale Leitung (z. B. eine T1-PRI-Leitung) mit einem an einen analogen Anschluß angeschlossenen Modem zu kommunizieren. Ankommende Modemrufe und ankommende Datenrufe werden über ein und dieselbe digitale Leitung übertragen.

Die MAX-Einheit kann ankommende Rufe aus dem Netz entweder als reinen digitalen Datenstrom oder als PCM-codierten (Pulse Coded Modulation) digitalen Datenstrom empfangen. PCM-codierte digitale Ströme enthalten eine digitalisierte Version der von einem Anrufer mit einem Modem gesendeten analogen Wellenform. Die MAX-Einheit kann abgehende Daten in analoge Wellenformen umwandeln, diese Wellenformen in einen PCM-codierten

digitalen Strom konvertieren und diesen dann über eine digitale Leitung zum Netz senden. Das Netz präsentiert diese Daten dem antwortenden Modem über eine analoge Leitung in analoger Form. Die Daten sehen genau so aus, wie sie erscheinen würden, wenn sie von einem analogen Modem gesendet worden wären.

digitales Signal – Signaltyp, der die über einen Draht gesendeten Daten mit einer begrenzten Zahl von diskreten Werten verschlüsselt. Der Wert der im digitalen Signal verschlüsselten Daten hängt vom Status des Signals während eines bestimmten Zeitabschnitts ab. Daher müssen sowohl der Sender als auch der Empfänger ihre internen Uhren synchronisieren. Jede Uhr läuft mit einer bestimmten Baudrate, die angibt, wie oft der Status des Signals pro Sekunde gelesen oder festgesetzt wird. Es gibt verschiedene Taktgeberverfahren, und digitale Signale verfügen häufig über Taktzeitgeber-Achtungssignale.

Digitale Signale können zur Übertragung von analogen oder digitalen Daten verwendet werden. So werden z. B. auf einer CD analoge Musikdaten in digitalen Signalen verschlüsselt, während die Kabel zwischen zwei Computern digitale Daten in digitalen Signalen übertragen.

D-Kanal – Kanal, über den WAN-Synchronisierungs- und Zeichengabeinformationen übertragen werden.

DLCI – *Data Link Connection Identifier.* DLCIs dienen in Frame-Relay-Netzwerken zur eindeutigen Kennzeichnung der virtuellen Schaltungen. In den meisten Fällen haben DLCIs nur für die jeweilige Frame-Relay-Schnittstelle Bedeutung.

DNS – *Domain Name System.* TCP/IP-Dienst, mit dessen Hilfe statt einer IP-Adresse ein aussagekräftigerer symbolischer Name festgelegt werden kann. Symbolische Namen bestehen aus einem Benutzernamen und einem Domänennamen. Sie haben das Format *benutzername@domänenname*. Der *benutzername* entspricht der Hostnummer in der IP-Adresse, während der *domänenname* der Netzwerknummer in der IP-Adresse entspricht. Symbolische Namen können z. B. wie folgt aussehen: maja@abc.com oder chris@xyz.edu. Der letzte Teil des Domänennamens ist die Domänenkennung, die angibt, zu was für einer Art von Unternehmen der Host gehört.

DNS unterhält auf einem Domänennamenserver eine Datenbank mit Netzwerknummern und den entsprechenden Domänennamen. Wenn Sie einen symbolischen Namen verwenden, übersetzt DNS den Domänennamen in eine IP-Adresse und sendet diese über das Netz. Beim Internet-Service-Provider wird

dann mit Hilfe einer eigenen Datenbank der der Hostnummer entsprechende Benutzername gesucht.

Domänenkennung – Der Teil eines Domänennamens, der als letztes erscheint und angibt, zu welcher Art von Organisation der Host gehört. Diese Domänenkennungen werden vom Internet-Network Information Center (NIC) zur Verfügung gestellt:

Domänenkennung	Erklärung
.arpa	ARPANET
.com	kommerzielles Unternehmen
.edu	Bildungseinrichtung
.gov	Regierungseinrichtung oder Behörde
.mil	militärische Organisation
.org	andere Organisation

Domänenname – Der Teil eines symbolischen Namens, der der Netzwerknummer in der IP-Adresse entspricht. Beim symbolischen Namen „stefan@abc.com“ lautet der Domänenname „abc.com“.

DS0 – 64-KBit/s-Einheit der Übertragungsbandbreite. DS0 ist ein weltweit gültiger Standard für die Digitalisierung von Telefongesprächen (Sprachrufe) und seit einiger Zeit auch für die Datenübertragung. 24 DS0 (24 x 64 KBit/s) entsprechen einem DS1.

DTE – *Data Terminal Equipment* (Datenendeinrichtung). Gemäß der RS-232-Spezifikation eine Einrichtung, die mit einer Datenendeinrichtung (Data Communications Equipment, DCE), z. B. einem PC oder einem Datenendgerät, verbunden ist. DTEs sind oft Anwendungsgeräte, wie z. B. Videokonferenz-Terminals oder LAN-Bridges bzw. -Router, während es sich bei DCEs zum Beispiel um Netzzugangseinrichtungen handelt.

Dual-Port-Ruf – Ruf, bei dem der serielle Host (z. B. ein Video-Codec) Invers-Multiplexing auf zwei Kanälen ausführt, so daß dem Ruf im Vergleich zu Einkanalrufen die doppelte Bandbreite zur Verfügung steht. Der serielle Host verfügt

über zwei Anschlüsse, für jeden der beiden Kanäle einen. Der Dual-Port-Ruf wird über zwei serielle Anschlüsse an der MAX-Einheit, dem *primären Anschluß* und dem *sekundären Anschluß*, mit dem seriellen Host verbunden. Da die MAX-Einheit die beiden Rufe im Tandem initiiert und abschließt, werden sie als einzelner Ruf betrachtet.

E1-PRI-Leitung – ISDN-Leitung, die aus 32 64-KBit/s-Kanälen besteht. Diese 32 Kanäle werden wie folgt benutzt: 30 B-Kanäle für die Benutzerdaten, ein 64-KBit/s-D-Kanal für die ISDN-D-Kanal-Zeichengabe und ein Rahmenkanal. Die B-Kanäle können entweder alle gewählt, alle festgeschaltet oder aber sowohl gewählt als auch festgeschaltet sein. Diese Art von PRI-Leitungen ist ein in Europa und Asien verwendeter Standard namens CEPT G.703.

Ethernet – Lokales Netzwerk (LAN), mit dem Geräte wie Computer, Drucker und Terminals miteinander verbunden werden können. Ethernet verwendet Twisted-Pair- oder Koaxialkabel mit Geschwindigkeiten von 10 oder 100 MB/s.

Ethernet-Transceiver – Ethernet-Gerät zur Verbindung von Workstations mit standardmäßigen dicken oder dünnen Ethernet-Kabeln, das Informationen sendet und empfängt und oft auch in der Lage ist, Datenpaketkollisionen zu entdecken.

Fernverwaltung – Verwaltungsfunktion, die es Ascend-Einheiten erlaubt, über den durch das AIM-Protokoll (Ascend Inverse Multiplexing) hergestellten Verwaltungssubkanal Bandbreite zur Steuerung, Konfiguration und Anforderung statistischer und diagnostischer Informationen über eine jede andere Ascend-Einheit zu verwenden. Mehrstufige Sicherheitseinrichtungen sorgen dafür, daß Unbefugte keinen Zugang zu Fernverwaltungsfunktionen haben. Englische Bezeichnung: *Remote Management*.

Fernzugriff – Möglichkeit, von Zweigstellen, Heimarbeitsplätzen und mobilen Computern aus über digitale oder analoge Stand- oder Wählleitungen auf das Unternehmens-LAN zuzugreifen. Englische Bezeichnung: *Remote Access*.

Festverbindung – Permanente Verbindung zwischen Endpunkten, über die die zwei Seiten Daten austauschen können. Festverbindungen werden auch als *Mietleitungen*, *gemietete Leitungen* oder *Standleitungen* bezeichnet.

Filter – Regeln, die definieren, welche Pakete über das Netzwerk weitergeleitet werden. Um festzulegen, was mit den Paketen geschehen soll, können Filter Zieladressen, Ausgangsadressen oder Protokolle überprüfen. Einer der Header des Pakets muß Informationen enthalten, die mit den Angaben in den Filterregeln (Filterkriterien) übereinstimmen; andernfalls wird das Paket ausgesondert. Siehe auch „Firewall“, „Secure Access Firewall“, „SAM“.

Firewall – Hardware/Software-Werkzeug, mit dessen Hilfe der Netzwerkadministrator feststellen kann, welche Benutzergruppen auf die Ressourcen im Netzwerk zugreifen können. Der Firewall ist Mechanismus zur Überwachung von Daten von autorisierten Benutzern (und nur von diesen) und zum Durchschleusen dieser Daten zum oder vom Netzwerk. Ein Firewall kann z. B. ein Software-Programm sein, das auf einer UNIX-Plattform oder einer anderen Plattform läuft. Er kann aber auch Teil eines proprietären Betriebssystems sein. Der Firewall selbst übernimmt keine Routing-Funktion. Siehe auch „Filter“, „Secure Access Firewall“, „SAM“.

Frame Relay – Form der Paketvermittlung, bei der kleinere Pakete und weniger Fehlerkorrekturmaßnahmen verwendet werden als bei herkömmlichen Formen der Paketvermittlung (wie z. B. X.25). Jetzt internationaler Standard für die effiziente Hochgeschwindigkeits-Übertragung von in Blöcken aufgeteilten Daten über WANs.

gemietete Leitungen, **Mietleitungen** – Schaltung, die von einer Telefongesellschaft für die exklusive Nutzung rund um die Uhr und an sieben Tagen der Woche gemietet wurde. Dabei werden zwei zuvor bestimmte Punkte miteinander verbunden und es kann nicht auf andere Ziele umgeschaltet werden.

Geradeauskabel – Kabel mit Drähten, bei denen die Anschlußbelegung auf beiden Seiten des Kabels identisch ist.

H0-Kanal – Beim „Switched-384“-Datendienst eine aus 6 B-Kanälen oder 384 KBit/s bestehende Schaltung.

H11-Kanal – Beim „Switched-1536“-Datendienst eine aus 24 B-Kanälen oder 1536 KBit/s bestehende Schaltung.

HDLC – *High-level Data Link Control*. Synchrones, bitorientiertes Verbindungsschichtenprotokoll für die Datenübertragung. Ein Beispiel für ein Paketprotokoll auf HDLC-Basis ist Frame Relay.

Host – Computer in einem Netzwerk.

IEEE – *Institute of Electrical und Electronics Engineers*. Amerikanische Organisation, die die Standards für 10BaseT-Netzwerke sowie andere Kommunikationsstandards definiert.

Inband-Zeichengabe – Art der Zeichengabe, bei der die Leitung 8 KBit/s jedes 64-KBit/s-Kanals für die WAN-Synchronisierung und Zeichengabe verwendet. Die übrigen 56 KBit/s stehen zur Übertragung von Benutzerdaten zur Verfügung.

Inband-Zeichengabe wird von T1-Zugangsleitungen mit einem oder mehreren gewählten Kanälen sowie von „Switched-56“-Leitungen verwendet.

Invers-Multiplexer – Gerät, daß an jedem Ende einer Verbindung Invers-Multiplexing durchführt.

Invers-Multiplexing – Verfahren, bei dem einzeln gewählte Kanäle in einem einzigen Datenstrom mit höherer Geschwindigkeit zusammengefaßt werden. Auf beiden Seiten der Verbindung kommt ein *Invers-Multiplexer* zum Einsatz.

Stellen Sie sich z. B. vor, an einem Ort sind drei ISDN-Basisanschlußleitungen mit einem Invers-Multiplexer verbunden und an einem anderen Ort ist eine T1-Zugangsleitung ebenfalls an einen Invers-Multiplexer angeschlossen. Der Benutzer auf der ersten Seite kann mit Hilfe des Invers-Multiplexing einen 336-KBit/s-Ruf für die andere Seite initiieren. Da jede BRI-Leitung über zwei 64-KBit/s-Kanäle verfügt (jeweils 56 KBit/s davon sind für Daten reserviert), initiiert der Invers-Multiplexer sechs einzelne Rufe über „Switched-56“-Dienste zum Invers-Multiplexer der antwortenden T1-Leitung. Die beiden Invers-Multiplexer fassen die sechs Rufe in einem einzigen Datenstrom mit 336 KBit/s (6 x 56 /s) zusammen.

Es gibt zwei Arten des Invers-Multiplexings: *Invers-Multiplexing auf Paketebene* und *Invers-Multiplexing auf Schaltungsebene*.

Beim Invers-Multiplexing auf Paketebene arbeitet der Multiplexer auf der Paketebene und verwendet dazu das MP- oder das MPP-Protokoll. Ein Datenpaket wird über die erste Schaltung gesendet, das nächste über die zweite Schaltung und so weiter, bis alle Datenpakete über alle verfügbaren Schaltungen gesendet wurden. Auf der empfangenden Seite werden durch das Netzwerk bedingte Verzögerungen kompensiert und die Datenpakete wieder in der richtigen Reihenfolge zusammengestellt. Dieses Invers-Multiplexing-Verfahren wird auch als *Lastausgleich* bezeichnet. Invers-Multiplexing auf Paketebene wird von Telekommunikationsanwendungen verwendet.

Beim Invers-Multiplexing auf Schaltungsebene teilt der Invers-Multiplexer den Datenstrom in gleich große Teile auf und sendet jeden dieser Teile über eine verfügbare Schaltung. Das empfangende Ende wartet netzwerkbedingte Verzögerungen ab und stellt die einzelnen Datenpakete wieder in der richtigen Reihenfolge zusammen. Die Arbeitsweise des Invers-Multiplexing auf Schaltungsebene wird durch die Protokolle AIM und BONDING definiert. Das inverse Multiplexing auf Schaltungsebene wird für Anwendungen benötigt, die

transparente digitale Schaltungen erfordern. Dazu gehören Videokonferenz-Systeme, festgeschaltete Backup- und Überlaufanwendungen sowie Anwendungen für die Übertragung großer Datenmengen.

Invers-Multiplexing auf Paketebene – Invers-Multiplexing-Verfahren, bei dem der Invers-Multiplexer seine Funktion auf der Paketebene ausführt und dazu das Protokoll MP oder MPP verwendet. Ein Datenpaket wird über die erste Schaltung gesendet, das nächste über die zweite Schaltung und so weiter, bis alle Datenpakete über alle verfügbaren Schaltungen gesendet wurden. Auf der empfangenden Seite werden durch das Netzwerk bedingte Verzögerungen kompensiert und die Datenpakete wieder in der richtigen Reihenfolge zusammengestellt. Dieses Invers-Multiplexing-Verfahren wird auch als *Lastausgleich* bezeichnet. Invers-Multiplexing auf Paketebene wird von Telearbeitsanwendungen verwendet.

Invers-Multiplexing auf Schaltungsebene – Invers-Multiplexing-Verfahren, bei dem der Invers-Multiplexer den Datenstrom in gleichgroße Teile aufteilt und jeden dieser Teile über eine verfügbare Schaltung überträgt. Das empfangende Ende wartet netzwerkbedingte Verzögerungen ab und stellt die einzelnen Datenpakete wieder in der richtigen Reihenfolge zusammen. Die Arbeitsweise des Invers-Multiplexing auf Schaltungsebene wird durch die Protokolle AIM und BONDING definiert. Das inverse Multiplexing auf Schaltungsebene wird für Anwendungen benötigt, die transparente digitale Schaltungen erfordern. Dazu gehören Videokonferenz-Systeme, festgeschaltete Backup- und Überlaufanwendungen sowie Anwendungen für die Übertragung großer Datenmengen.

IP-Adresse – Adresse, mit der jeder Host in einem Netzwerk oder im Internet eindeutig gekennzeichnet werden kann.

Eine IP-Adresse ist 32 Bits lang und in vier Teile zu jeweils 8 Bits unterteilt, die jeweils durch einen Punkt voneinander getrennt sind (Beispiel: 149.122.3.30). Diese Schreibweise wird auch *Dezimalnotation mit Punkten* genannt. Jeder der vier Teile der Adresse kann einen Wert zwischen 1 und 255 haben.

IP-Adressen bestehen aus einer *Netzwerknummer* und einer *Hostnummer.* Es gibt drei Arten von IP-Adressen: Klasse A, Klasse B und Klasse C. Die Klasse der IP-Adresse bestimmt, welcher Teil der Adresse zur Netzwerknummer und welcher Teil zur Hostnummer gehört. Die Klasse wird mit den ersten Bits der IP-Adresse gekennzeichnet. Die Klasse des Netzwerks wird vom Internet-Network Information Center (NIC) festgelegt.

Adressen der Klasse A beginnen mit 0 als Klassenkennung. Es schließen sich 7 Bits für die Netzwerknummer und 24 Bits für die Hostnummer an. Daher ist die erste Zahl in der IP-Adresse die Netzwerknummer und die nächsten drei Zahlen repräsentieren die Hostnummer. So ist in der IP-Adresse 127.120.3.8 „127“ die Netzwerknummer und „120.3.8“ die Hostnummer. Diese Adressenart wird von den größten Organisationen verwendet, da auf diese Weise mehr als 16 Millionen verschiedene Hostnummern möglich sind. Die Netzwerknummern können jedoch auch nur einen Wert von maximal 128 haben.

Adressen der Klasse B beginnen mit einer binären 10 als Klassenkennung. Es schließen sich 14 Bits für die Netzwerknummer und 16 Bits für die Hostnummer an. Daher bilden die ersten beiden Zahlen der Adresse die Netzwerknummer, während die Hostnummer durch die zweiten beiden Zahlen repräsentiert wird. So ist in der IP-Adresse 147.14.86.24 „147.14“ die Netzwerknummer und „86.24“ die Hostnummer. Bei Adressen der Klasse B sind mehr Netzwerknummern, aber weniger Hostnummern verfügbar (ca. 65.000).

Adressen der Klasse C beginnen mit einer binären 110 als Klassenkennung. Es schließen sich 21 Bits für die Netzwerknummer und 9 Bits für die Hostnummer an. Daher bilden die ersten drei Nummern der Adresse die Netzwerknummer, während die Hostnummer durch die letzte Zahl repräsentiert wird. So ist in der IP-Adresse 225.135.38.42 „225.135.38“ die Netzwerknummer und „42“ die Hostnummer. Bei Adressen der Klasse C sind viele Netzwerknummern verfügbar, jedoch nur 254 Hostnummern pro Netzwerknummer. Die Zahlen 0 und 255 sind reserviert.

Zu welcher Klasse eine IP-Adresse gehört, können Sie erkennen, wenn Sie sich den ersten 8-Bit-Teil der Adresse ansehen. Adressen der Klasse A beginnen mit einer Zahl zwischen 0 und 127, Adressen der Klasse B mit einer Zahl zwischen 128 und 223 und Adressen der Klasse C mit einer Zahl zwischen 192 und 233.

Neben der IP-Adresse können Sie auch einen von DNS (Domain Name Services) bereitgestellten symbolischen Namen verwenden, um eine Internet-Adresse anzugeben.

IP-Subnetz – IP-Subnetze oder Subnetzmasken stellen eine Möglichkeit dar, ein Netzwerk in kleinere Netze aufzuteilen, so daß eine größere Zahl von Computern mit einer gemeinsamen IP-Adresse angeschlossen werden können. Das IP-Subnetz ist eine Zahl, die an die IP-Adresse angehängt wird. So haben die IP-Adressen 195.112.56.75/14, 195.112.56.75/15 bzw. 195.112.56.75/16 die Subnetze (Subnetzmasken) 14, 15 bzw. 16.

ISDN – *Integrated Services Digital Network*, dt.: diensteintegrierendes Digitalnetz. System zur gleichzeitigen Hochgeschwindigkeitsübertragung von Sprache und Daten über einen einzigen Kanal zum Teilnehmeranschluß. ISDN ist ein internationaler Standard für die digitale Ende-zu-Ende-Übertragung von Sprache, Daten und Zeichengabeinformationen.

ISDN-Basisanschluß – Leitung, die zwei B-Kanäle für die Benutzerdaten und einen 16-KBit/s-D-Kanal für die ISDN-D-Kanal-Zeichengabe verwendet. Die B-Kanäle können beide gewählt, beide festgeschaltet oder aber der eine gewählt und der andere festgeschaltet sein. Über Leitungen dieser Art können Verbindungen zu Standard-Sprachdiensten, zu einem „Switched-56"-Dienst oder zu einem „Switched-64"-Datendienst aufgebaut werden.

ISDN-D-Kanal-Zeichengabe – Art der Zeichengabe, bei der ein D-Kanal für die WAN-Synchronisierung und Zeichengabe verwendet wird und die B-Kanäle zur Übertragung der Benutzerdaten verwendet werden. Die ISDN-D-Kanal-Zeichengabe wird auch als *Außerband-Zeichengabe* bezeichnet. Die ISDN-D-Kanal-Zeichengabe wird von T1-PRI-, E1-PRI- und ISDN-Basisanschlußleitungen verwendet.

Kanäle – Teil der Bandbreite einer Leitung. Leitungen enthalten eine feste Anzahl von Kanälen. Jede Leitung kann entweder nur gewählte Kanäle, nur festgeschaltete Kanäle oder aber eine Mischung aus gewählten und festgeschalteten Kanälen haben.

Leitungen können die folgenden Kanalarten enthalten:

- DS0

  Der DS0-Kanal ist ein 64-KBit/s-Kanal einer Leitung mit Inband-Zeichengabe. Informationen zur Inband-Zeichengabe finden Sie unter „Inband-Zeichengabe".

- B-Kanal

  Ein B-Kanal ist ein 56-KBit/s- oder 64-KBit/s-Kanal, über den die Benutzerdaten auf einer Leitung mit ISDN-D-Kanal-Zeichengabe übertragen werden. Informationen zur ISDN-D-Kanal-Zeichengabe finden Sie unter „ISDN-D-Kanal-Zeichengabe".

- D-Kanal

  Der D-Kanal dient zur Übertragung der WAN-Synchronisierungsinformationen auf einer Leitung mit ISDN-D-Kanal-Zeichengabe. Informationen zur ISDN-D-Kanal-Zeichengabe finden Sie unter „ISDN-D-Kanal-Zeichengabe".

LAN – *Local Area Network* (lokales Netzwerk). Netzwerk, das Geräte über einen geographisch eng begrenzten Raum, meistens innerhalb eines Gebäudes oder eines Teils eines Gebäudes, miteinander verbindet. Der verbreitetste LAN-Typ ist Ethernet, ein 10-MB/s-Standard, bei dem 10BaseT-, 10Base2- oder 10Base5-Kabel verwendet werden. Wenn Sie die Pipeline mit Hilfe des mitgelieferten Crossover-Kabels mit einem nicht an ein Netzwerk angeschlossenen PC verbinden, haben Sie ein aus zwei Knoten bestehendes Ethernet-Netzwerk aufgebaut.

Leitung – Physikalische Schnittstelle zum WAN.

Local Area Network – Siehe „LAN“.

lokales Netzwerk – Siehe „LAN“.

LQM – *Line Quality Monitoring* (Überwachung der Leitungsqualität) – Leistungsmerkmal, mit dem die Ascend-Einheit in die Lage versetzt wird, die Qualität einer Verbindung zu überwachen.

Dabei wird die Anzahl der über die Verbindung gesendeten Pakete gezählt und das entfernte Ende in regelmäßigen Abständen gefragt, wie viele Pakete bei ihm angekommen sind. Sind die beiden Werte unterschiedlich, läßt dies auf den Verlust von Paketen und damit auf Probleme mit der Verbindungsqualität schließen. Wenn die Probleme einen festgelegten Grenzwert überschreiten, kann die Ascend-Einheit den Ruf abbrechen und ihn erneut aufbauen.
Mietleitung – Siehe „gemietete Leitungen“.

Modem – *MOdulator/DEModulator.* Datenübertragungseinrichtung (DCE), die zwischen einer Datenendeinrichtung (DTE) und einem analogen Übertragungskanal, wie z. B. einem Telefonanschluß, installiert ist. Bei der Datenendeinrichtung kann es sich z. B. um einen Computer oder ein Terminal handeln. Die Datenübertragungseinrichtung (das Modem) verbindet die Datenendeinrichtung mit einem Übertragungskanal, wie z. B. einem Telefonanschluß. Das Modem empfängt die von der Datenendeinrichtung gesendeten digitalen Daten, übersetzt (moduliert) die Einsen und Nullen in das analoge Format und sendet die Daten über den Kanal weiter. Das Modem auf der anderen Seite der Verbindung wandelt das analoge Signal wieder in digitale Daten um (Demodulierung) und sendet sie zur Datenendeinrichtung, an die es angeschlossen ist.

MP – *Multilink PPP.* Vorgeschlagener Standard für das inverse Multiplexing, einem Verfahren zur Zusammenfassung einzeln gewählter Kanäle in einem einzigen Datenstrom mit höherer Geschwindigkeit. MP ist eine Erweiterung des Protokolls PPP und unterstützt das Versenden und Sortieren von Datenpaketen über mehrere Kanäle.

MPP – *Multichannel Point-to-Point Protocol*. Protokoll, das die Fähigkeiten von MP um die Unterstützung des Invers-Multiplexing, des Sitzungsmanagements und des Bandbreitenmanagements erweitert. MPP ermöglicht die Zusammenfassung von bis zu 30 einzelnen Kanälen zu einer gemeinsamen Hochgeschwindigkeitsverbindung.

MPP besteht aus zwei Komponenten: eine untere Ebene zur Kanalerkennung, Fehlerüberwachung und Fehlerbeseitigung und eine Sitzungsmanagementebene für Bandbreitenänderungen und Diagnosetests. MPP versetzt die Ascend-Einheit in die Lage, einer Verbindung entsprechend dem jeweiligen Bandbreitenbedarf Kanäle hinzuzufügen oder zu entziehen, ohne daß dabei die Verbindung unterbrochen wird. Diese Funktion wird dynamische Bandbreitenzuweisung (Dynamic Bandwidth Allocation, DBA) genannt.
MPP muß sowohl von der wählenden als auch von der antwortenden Seite unterstützt werden. Wird MPP nur von einer Seite unterstützt, verwendet die Verbindung MP oder das standardmäßige Einkanal-PPP.

Das Kombinieren eines ISDN-Basisanschlußkanals mit einer T1-Zugangsleitung bzw. einer T1-PRI-Leitung ist bei MPP-Rufen nicht möglich.
MultiRate – Datendienst, der aus einer einzelnen Schaltung besteht, deren Bandbreite ein Vielfaches von 64 KBit/s ist. Diese Schaltung besteht aus einem oder mehreren B-Kanälen. So läßt sich z. B. ein erster Ruf mit 384 KBit/s (über 6 B-Kanäle) und dann ein zweiter Ruf mit 512 KBit/s (über 8 B-Kanäle) wählen. Dieser Dienst steht nur über T1-PRI-Leitungen zur Verfügung. Der MultiRate-Datendienst wird auch „Switched Nx64“-Datendienst genannt.

NFAS – *Non-Facility Associated Signalling*. Spezieller Fall der ISDN-Zeichengabe, bei dem zwei oder mehr T1-PRI-Leitungen denselben D-Kanal benutzen und der Benutzer einen Backup-D-Kanal hinzufügen kann. NFAS wird für den „Switched-1536“-Datendienst benötigt; da alle 24 Kanäle der T1-PRI-Leitung für Benutzerdaten verwendet werden, muß der D-Kanal auf einer anderen Leitung sein.

NT1 – Ein Leitungsabschlußgerät für ISDN-Basisanschlüsse beim Teilnehmer, das die S0-Schnittstelle für die Leitungswartung, die Zeitschaltung und die Echokompensation bereitstellt. NT1-Abschlußgeräte können auch in andere Ausrüstungskomponenten integriert sein.

Oktett – Acht Datenbits.

PAP – *Password Authentication Protocol*. Sicherheitsprotokoll, das den Zugang zum Netzwerk oder Host über Kennwörter steuert.

Parität – Bei der 7-Bit-Kommunikation sendet jedes Gerät nur die ersten 128 Zeichen im ASCII-Zeichensatz, da diese Zeichen jeweils mit maximal sieben Bits dargestellt werden können. Mit Hilfe der Parität kann das Gerät bestimmen, ob es die Daten genau so erhalten hat, wie sie vom sendenden Gerät gesendet wurden. Jedes Gerät muß festlegen, ob es gerade Parität, ungerade Parität oder keine Parität verwendet.

Das sendende Gerät addiert die Einsen in jeder von ihm gesendeten Zeichenkette und überprüft, ob die Summe gerade oder ungerade ist. Dann wird der Zeichenkette ein zusätzliches Bit, das sogenannte Paritätsbit hinzugefügt. Wird gerade Parität verwendet, sorgt das Paritätsbit dafür, daß die Summe der Bits gerade wird. Bei ungerader Parität macht das Paritätsbit die Summe der Bits ungerade. Wenn ein Gerät z. B. die Binärzahl 1010101 bei gerader Parität sendet, hängt es an das Ende des Bytes eine 0 (Null) an, da die Summe der Einsen bereits gerade ist. Wird die gleiche Zahl dagegen bei ungerader Parität gesendet, wird statt der 0 eine 1 an das Ende des Bytes angehängt, damit die Summe der Einsen ungerade wird.

Das empfangende Gerät überprüft, ob die Summe der Einsen in einem Zeichen gerade oder ungerade ist. Verwendet das Gerät gerade Parität, muß die Summe der Einsen im Zeichen gerade sein. Verwendet das Gerät ungerade Parität, muß die Summe der Einsen im Zeichen ungerade sein. Wenn die Summe der Bits nicht mit der Paritätseinstellung übereinstimmt, weiß das empfangende Gerät, daß bei der Übertragung der Daten ein Fehler aufgetreten ist.

Die ASCII-Sonderzeichen (128–256) können nur mit acht Bits dargestellt werden. Bei der 8-Bit-Kommunikation wird kein Paritätsbit verwendet.
Nebenstellenanlage – Siehe „Tk-Anlage“.

PBX – *Private Branch Exchange*. Siehe „Tk-Anlage“.

POST – *Power-On Self Test* (Selbsttest beim Einschalten). Diagnosetest, den die Ascend-Einheit beim Einschalten oder nach einer Rücksetzung des Systems ausführt. Während des Selbsttests, bei dem die Ascend-Einheit den Hauptspeicher des Systems, die Konfiguration, die installierten Module und die T1-Verbindungen überprüft, leuchtet die gelbe „FAULT“-LED auf. Besteht die Ascend-Einheit einen der Tests nicht, leuchtet die „FAULT“- (oder die „CON“-)LED konstant weiter oder blinkt.

PPP – *Point-to-Point Protocol*. Standardprotokoll, das die Einkapselung der Datenpakete ermöglicht, die über eine Einkanal-WAN-Verbindung gesendet wer-

den sollen. PPP ist das Standard-WAN-Einkapselungsprotokoll für das gegenseitige Zusammenwirken von Bridges und Routern. PPP wird auch in an das Netzwerk angeschlossenen Arbeitsplatzcomputern unterstützt, wo es den direkten Einwählzugang von einem PC zu einem Unternehmens-LAN oder zu einem Internet-Service-Provider ermöglicht. Die Verwendung von PPP gewährleistet die grundlegende Kompatibilität mit nicht von Ascend stammenden Geräten. PPP muß sowohl von der wählenden als auch von der antwortenden Seite unterstützt werden.

promiskuitiver Modus – Bridging-Parametermodus, in dem der Ethernet-Controller in der Ascend-Einheit alle Pakete innerhalb des Protokollstapels weiterleitet und damit die Entscheidung, ob das jeweilige Paket geroutet, überbrückt oder abgewiesen werden soll, einer höheren Ebene überläßt. Dieser Modus ist dann geeignet, wenn die Ascend-Einheit als Bridge verwendet wird.

Protokoll – Gruppe von Regeln für den Austausch von Meldungen über ein Netzwerk bzw. zwischen Netzwerken. Zu den verbreitetsten Protokollen gehören TCP/IP (Transmission Control Protocol/Internet Protocol), PPP (Point-to-Point Protocol) und IPX (Internet Packet Exchange).

RADIUS – *Remote Access DIalup User Service*. Protokoll, mit dessen Hilfe Benutzer über einen zentral verwalteten Server auf gesicherte Netzwerke zugreifen können. RADIUS ermöglicht die Autorisierung für eine Reihe verschiedener Dienste, wie z. B. Anmelden, Rückruf, SLIP und PPP.

In einer RADIUS-Anfrage sendet die MAX-Einheit dem Server eine Benutzerkennung und ein Kennwort. Der Server sendet ein komplettes Profil zurück, in dem Festlegungen für das Routing, das Filtern von Paketen, zielspezifische statische Routen und benutzerspezifische Nutzungseinschränkungen enthalten sind. Die MAX-Einheit kann die Daten in der RADIUS-Datenbank auch dazu nutzen, statische Routen zu erstellen und bekanntzumachen sowie abgehende Rufe zu initiieren.

Der Kommunikationskanal zwischen RADIUS-Client und -Server wird von UDP/IP zur Verfügung gestellt, wobei Meldungen quittiert werden. Der Hauptvorteil bei der Verwendung von RADIUS zur Autorisierung ankommender Rufe besteht darin, daß Sie alle Benutzerinformationen offline auf einem separaten Server auf UNIX-Basis speichern können. Praktisch alle Verbindungsprofilinformationen werden auf dem RADIUS-Server in einer ASCII-Datenbank gespeichert. Dieser Server ist in der Lage, Autorisierungsanforderungen von vielen Computern gleichzeitig zu verarbeiten,

wodurch der Wechsel von einem Einwähl-Netzwerkserver zu einem anderen wesentlich vereinfacht wird.
Remote Access – Siehe „Fernzugriff“.

Remote Management – Siehe „Fernverwaltung“.

RFC – *Request For Comments*. 1969 begonnene Reihe von Dokumenten, die die Internet-Protokolle und damit in Zusammenhang stehende Experimente beschreiben. Nicht alle (sogar nur sehr wenige) RFCs beschreiben Internet-Standards, aber alle Internet-Standards sind als RFCs geschrieben. Die RFC-Dokumentreihe ist insofern ungewöhnlich, als daß die Protokollvorschläge, im Gegensatz zu den formell überarbeiteten und standardisierten Protokollen großer Organisationen, wie CCITT oder ANSI, von den Leuten, die sich mit den Internet-Problemen beschäftigen, in deren eigenem Namen über das Internet verbreitet werden. Eine vollständige Liste der RFCs finden Sie unter der WWW-Adresse http://www.internic.net/rfc/.

Router – Gerät, mit dessen Hilfe mehrere einzelne LANs miteinander verbunden werden können. Im Gegensatz zu Bridges, die logische Verbindungen in der OSI-Schicht 2 herstellen, stellen Router logische Wege in der OSI-Schicht 3 her. Router können, wie Bridges, zur Verbindung von entfernten Standorten über Stand- oder Wählleitungen verwendet werden, wodurch ein WAN entsteht.

Routing – Gerät oder Einrichtung, das die beste Route zwischen zwei beliebigen Netzwerken findet, auch wenn dazu mehrere Netzwerke zu durchqueren sind. (Gegenteil: Bridging).

RS-232 – Gruppe von EIA-Standards, in denen verschiedene elektrische und mechanische Merkmale für Schnittstellen zwischen Datenend- und Datenübertragungseinrichtungen (DTEs und DCEs) definiert sind. Der Standard gilt für die synchrone und die asynchrone Übertragung binärer Daten mit einer Geschwindigkeit von unter 64 KBit/s.

Rückschleife – Test, bei dem die Ascend-Einheit einen Ruf an sich selbst über das WAN initiiert und diese Verbindung zur Übertragung einer vom Benutzer angegebenen Anzahl von Paketen benutzt. Dabei wird die Fähigkeit der Ascend-Einheit getestet, Rufe zu initiieren und zu empfangen. Außerdem wird festgestellt, ob die Verbindung über die digitale Zugangsleitung und das WAN störungsfrei ist.

Ruf – Einzelsitzung, bei der über das WAN eine Verbindung zwischen dem rufenden Gerät und dem antwortenden Gerät hergestellt wird.

SAM – *Secure Access Manager.* SAM ermöglicht Netzwerkadministratoren die direkte detaillierte Steuerung der Sicherheitsfunktionen für das gesamte Netzwerk von einem zentralen Punkt aus. Mit Hilfe dieses Windows-Anwendungsprogramms können Netzwerkadministratoren die Option „Secure Access Firewall“ offline konfigurieren und die Konfiguration dann an entfernten Standorten herunterladen. Das menügestützte Programm ermöglicht die einfache und problemlose Konfiguration der Firewall-Einrichtungen für das Netzwerk.

Schaltung – Verbindung zwischen Endpunkten über ein physikalisches Medium.

Secure Access Firewall – „Secure Access Firewall“ ist eine Software-Option für Ascend-Einheiten, die eine vollständig integrierte Firewall-Sicherheit für den Zugriff auf entfernte Netzwerke bietet. Dabei kommen modernste dynamische Firewall-Verfahren zum Einsatz, um eine umfassende Sicherheitslösung für Unternehmens-LANs, LANs von Zweigstellen und Telearbeits-LANs zu bieten, die das Einbrechen von Eindringlingen verhindert. Durch die Sicherung der Grenzen des lokalen Netzwerks zum Internet wird die Nutzung des Internets für Intranet-Anwendungen möglich.

Sitzung – Der Zustand, den eine Verbindung eingenommen hat, wenn beide Seiten miteinander kommunizieren können.

SLIP – *Serial Line IP.* Protokoll, das Ihren Computer in die Lage versetzt, IP-Pakete über eine serielle Verbindung zu versenden und zu empfangen.

SMDS – *Switched Multimegabit Data Service*. Netzwerkdienst auf Paketbasis, mit dem Hochgeschwindigkeits-Datennetze (bis zu 45 MBit/s) aufgebaut werden können. Befindet sich gegenwärtig in der Erprobungsphase bzw. wird bereits in einigen Ländern eingesetzt.

SNMP – *Simple Network Management Protocol*. Standardmethode zur gemeinsamen Nutzung von Netzwerkinformationen durch mehrere Computer.

In SNMP gibt es zwei Arten von Kommunikationsgeräten: *Agents* und *Managers*. Ein Agent stellt der Manageranwendung auf einem anderen Computer Netzwerkinformationen zur Verfügung. Die Agents und Managers nutzen eine gemeinsame Informationsdatenbank, die *Management Information Base* (MIB). Ein Agent kann mit Hilfe einer *Traps-PDU* genannten Meldung freilaufende Informationen zum Manager senden.

Die MAX-Einheit unterstützt die SNMP-MIB II, die T1-MIB und die Ascend-Enterprise-MIBs. Sie können also die MAX-Einheit von einem zentralen SNMP-Manager, wie z. B. SunNet Manager™ oder HP Open View™, aus konfigurieren.

Da die WAN-Schnittstelle in die MAX-Einheit integriert ist, können Sie sie mit Hilfe der SNMP-T1-MIB und der Ascend-Enterprise-MIB verwalten. Die meisten anderen WAN-Schnittstellenarten, wie z. B. Kanalgruppen, T1-Multiplexer und CSU/DSUs, können nicht in das SNMP einbezogen werden. Die MAX-Einheit kann Alarme, Gebührenerfassungs- und andere Verwaltungsinformationen an einen SNMP-Manager senden, ohne daß diese abgefragt werden müssen.

Die SNMP-Sicherheit ist über den *Community-Namen* gewährleistet, der mit jeder Anforderung gesendet wird. Ascend unterstützt zwei Community-Namen, einen mit Nur-Leserechten und einen mit Lese- und Schreibrechten für die MIB.
SPID – *Service Profile Identifier.* Diese Nummer wird von einer Telefonnummer abgeleitet und von Ihrem ISDN-Diensteanbieter (Telefongesellschaft) in der zentralen Vermittlung verwendet, um die ISDN-Dienste für Ihren ISDN-Anschluß festzustellen.

Switched-56 – Datendienst, der aus einem einzigen 56-KBit/s-Kanal besteht. Dieser Dienst steht für alle Leitungsarten zur Verfügung. Er ist der einzige Dienst, der für T1-Zugangsleitungen und „Switched-56“-Leitungen verfügbar ist.

Da „Switched-56“ der erste verfügbare Datendienst war, wurden sowohl der Dienst selbst als auch die Leitungen für den Zugriff auf diesen Dienst „Switched-56“ genannt. Heute kann jede Leitungsart den „Switched-56“-Datendienst nutzen, und es gibt neben „Switched-56“ auch noch andere Dienste.
Switched-56-Leitung – Leitung, die einen einzelnen 56-KBit/s-Datenkanal mit Inband-Zeichengabe zur Verfügung stellt.

Switched-64 – Datendienst, der aus einem einzelnen 64-KBit/s-Kanal besteht. Dieser Dienst ist nur über T1-PRI-Leitungen und ISDN-Basisanschlüsse verfügbar.

Switched-384 – Datendienst, der aus einer einzelnen 384-KBit/s-Schaltung, dem sogenannten *H0-Kanal* besteht. Der H0-Kanal setzt sich aus 6 B-Kanälen zusammen. Dieser Dienst ist nur über T1-PRI-Leitungen verfügbar. „Switched-384“ ist auch unter dem Namen *H0*-Datendienst bekannt.

Switched-1536 – Datendienst, der aus einer einzelnen 1536-KBit/s-Schaltung, dem sogenannten *H11-Kanal* besteht. Der H11-Kanal setzt sich aus allen 24 Kanälen der Leitung zusammen. Für den Zugriff auf „Switched-1536“ sind zwei T1-PRI-Leitungen erforderlich: eine Leitung für die Benutzerdaten und die andere Leitung für den D-Kanal. Dieser Datendienst erfordert NFAS, da sich der D-Kanal auf einer separaten Leitung befinden muß. Dieser Dienst ist nur über

T1-PRI-Leitungen verfügbar. „Switched-1536“ wird auch als *H11*-Datendienst bezeichnet.

symbolischer Name – Name, der anstelle einer IP-Adresse verwendet wird. Ein symbolischer Name besteht aus einem Benutzernamen und einem Domänennamen. Er hat das Format *benutzername@domänenname*. Der *benutzername* entspricht der Hostnummer in der IP-Adresse, während der *domänenname* der Netzwerknummer in der IP-Adresse entspricht. Symbolische Namen können z. B. wie folgt aussehen: maja@abc.com oder chris@xyz.edu.

synchrone Übertragung – Übertragungsmodus, bei dem die Übertragung der Daten in großen Blöcken erfolgt, die Meldungen oder Rahmen genannt werden. Sowohl das sendende als auch das empfangende Gerät müssen die Synchronisierung aufrechterhalten, um bestimmen zu können, wo ein Datenblock endet und der nächste beginnt. Die Synchronisierung kann eine der folgenden Formen annehmen:

- Jede der beiden Seiten kann ein eigenes Synchronisierungssignal, den sogenannten Takt, senden.
- Die Synchronisierungsinformationen können in den einzelnen Rahmen bzw. Meldungen enthalten sein.

Bei der zweiten Methode beginnt jeder Datenblock mit einem oder mehreren SYNC genannten Steuerzeichen (im Normalfall 8 Bytes lang). Der Empfänger interpretiert das SYNC-Zeichen als ein Signal, das er mit dem Empfang von Daten beginnen kann. Die synchrone Übertragung ist bis zu 20 % schneller als das asynchrone Verfahren.

Synchronisierung – Verfahren bei der seriellen Datenübertragung, mit dem gewährleistet wird, daß die empfangende Seite Zeichen in der Reihenfolge erkennen kann, in der sie von der sendenden Seite gesendet wurden, und in der Lage ist festzustellen, wo ein Zeichen endet und das nächste anfängt. Ohne Synchronisierung würde die empfangende Seite Daten einfach nur als eine Folge von Bits ohne Beziehung zueinander ansehen.

T1-Leitung – Leitung, die aus 24 64-KBit/s-Kanälen besteht. Es gibt zwei Arten von T1-Leitungen: *T1-Zugangsleitungen* und *T1-PRI-Leitungen*.

T1-Leitung mit D4-Rahmen – T1-Leitung, die das D4-Format (oder Superframe-Format) verwendet, um Daten in der physikalischen Schicht „einzurahmen“. Das D4-Format besteht aus 12 aufeinanderfolgenden Rahmen, die jeweils durch Rahmenbits voneinander getrennt sind.

T1-PRI-Leitung – T1-Leitung, bei der 23 B-Kanäle für Benutzerdaten und ein 64-KBit/s-D-Kanal für die ISDN-D-Kanal-Zeichengabe verwendet wird. Bei den B-Kanälen dieser Leitung kann es sich entweder um nur gewählte Kanäle, um nur festgeschaltete Kanäle oder aber um sowohl festgeschaltete als auch gewählte Kanäle handeln. Diese Art der PRI-Leitung ist der Standard in Nordamerika, Japan und Südkorea. PRI ist die Abkürzung für *Primary Rate Interface*. Diese Leitungsart kann für Standard-Sprachrufe sowie für die Datendienste „Switched-56“, „Switched-64“, „Switched-384, „Switched-1536“ und MultiRate verwendet werden. Mit Hilfe der *PRI-zu-TI-Umwandlung* kann die MAX-Einheit sich die Bandbreite einer T1-PRI-Leitung mit einer Tk-Anlage teilen.

T1-Zugangsleitung – 1,544-MBit/s-T1-Leitung, die 24 56-KBit/s-Datenkanäle zur Verfügung stellt und mit Inband-Zeichengabe arbeitet. Bei den Kanälen dieser Leitung kann es sich entweder um nur gewählte Kanäle, um nur festgeschaltete Kanäle oder aber um sowohl festgeschaltete als auch gewählte Kanäle handeln. Diese Leitungsart kann für Standard-Sprachrufe sowie für den „Switched-56“-Datendienst verwendet werden. Mit Hilfe der *Drop-and-Insert*-Funktion kann die MAX-Einheit einen Teil der T1-Zugangsleitung für Datenzwecke verwenden und den verbleibenden Teil der Bandbreite der Leitung einer Tk-Anlage für Sprachrufe zur Verfügung stellen.

T3 – Digitale Übertragungsverbindung mit einer Kapazität von 45 Mbit/s bzw. 28 T1-Leitungen.

TACACS – *Terminal Access Concentrator Access Control Server.* Sehr einfaches Abfrage/Antwort-Protokoll, mit dem die MAX-Einheit das Kennwort eines Benutzers überprüfen und den Zugang gewähren oder aber verweigern kann. TACACS-Server unterstützen nur die grundlegenden Kennwortübermittlungen, die PAP verwenden. CHAP wird nicht unterstützt.

Tarif – Dokumente, die von einer unter staatlicher Aufsicht stehenden Telefongesellschaft bei der jeweiligen Aufsichtsbehörde eingereicht werden müssen und Auskunft über die Dienste, die Ausstattung und die Gebührenpolitik der Telefongesellschaft geben.

TCP/IP – *Transmission Control Protocol/Internet Protocol*. Gruppe von Protokollen, in denen das Format der über ein Netzwerk gesendeten Datenpakete definiert ist. TCP/IP ist der Kommunikationsstandard für die Datenübertragung zwischen verschiedenen Plattformen. Die TCP/IP-Familie besteht aus den folgenden Protokollen und Diensten:

- Transportprotokolle zur Steuerung der Datenübertragung zwischen Computern:
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)
- Routing-Protokolle zur Steuerung der Adressierung und Paketzusammensetzung sowie zur Festlegung der besten Routen für ein Paket zu dessen Ziel:
  - IP (Internet Protocol)
  - ICMP (Internet Control Message Protocol)
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First)
- Gateway-Protokolle ermöglichen es Netzwerken, auf gemeinsame Routing- und Statusinformationen zuzugreifen:
  - EGP (Exterior Gateway Protocol)
  - GGP (Gateway-to-Gateway Protocol)
  - IGP (Interior Gateway Protocol)
- Netzwerkadressendienste und -protokolle zur Festlegung, wie die Computer im Netzwerk gekennzeichnet und identifiziert werden:
  - DNS (Domain Name System)
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
- Benutzerdienste zur Bereitstellung von Anwendungen für den Benutzer:
  - BOOTP (Boot Protocol)
  - FTP (File Transfer Protocol)
  - Telnet
- weitere Dienste:
  - NFS (Network File System)
  - NIS (Network Information Service)
  - RPC (Remote Procedure Call)
  - SMTP (Simple Mail Transfer Protocol)
  - SNMP (Simple Network Management Protocol)

Teilnehmereinrichtung – Endgeräte am Standort des Teilnehmers, die für den Anschluß an das Telefonnetz verwendet werden. Englische Bezeichnung: CPE (Customer Premises Equipment).

Telearbeiter – Heimarbeiter am Computer, der über Fernzugriffsverfahren (z. B. mittels eines Modems über analoge Leitungen, eines ISDN-Terminaladapters oder ISDN-Routers über ISDN-Leitungen oder einer CSU/DSU über „Switched-56“-Leitungen) auf das Unternehmens-LAN zugreift.

Telnet – Protokoll, mit dem zwei Computer miteinander verbunden werden können, um eine Terminalverbindung zum entfernten Computer aufzubauen.

Statt sich in den Computer einzuwählen, wird mit Telnet eine Verbindung über das Internet hergestellt. Eine Telnet-Sitzung beginnen Sie, indem Sie eine Verbindung zum Telnet-Host herstellen und sich bei ihm anmelden. Wenn die Verbindung hergestellt ist, können Sie mit dem entfernten Computer arbeiten, als säßen Sie an einem mit diesem Computer verbundenen Terminal.

Wenn in Ihrer MAX-Einheit eine Ethernet-Karte installiert ist, können Sie die Einheit von einem entfernten Ort aus steuern, indem Sie von jeder beliebigen Telnet-Workstation im Netz eine Telnet-Verbindung herstellen und über ein Telnet VT-100-Fenster auf die MAX-Schnittstelle zugreifen. Telnet wird auch von allen Pipeline-Einheiten, mit Ausnahme der Pipeline 25, unterstützt.

IP-Hosts können Telnet zur Emulation eines Terminals benutzen. Wenn Sie die MAX-Einheit zur Initiierung einer Terminal-Server-Sitzung über Telnet oder den lokalen „Control/Console“-Anschluß verwenden, stehen der Sitzung ein Teil der Funktionen zur Verfügung, auf die eine Terminal-Server-Sitzung über eine asynchrone WAN-Verbindung zurückgreifen kann.

Terminal – Computer, der nicht über einen eigenen Prozessor verfügt und der eine asynchrone Verbindung zu einem Terminal-Server herstellen muß, um dessen Prozessor zu verwenden. Beispiele für Terminals sind VT100, ANSI und TTY.

Terminal-Emulator – Programm, mit dem Sie Ihren Computer wie ein Terminal aussehen lassen können, so daß eine Verbindung zu einem Terminal-Server aufgebaut werden kann. Während der Verbindung agiert Ihr Computer wie ein Terminal – sämtliche Verarbeitungsvorgänge werden am anderen Ende der Verbindung ausgeführt. Terminal-Emulatoren werden auch *Terminal-Emulationsprogramm* genannt.

Terminal-Server – Computer, mit dem ein Terminal eine Verbindung über ein LAN oder WAN herstellen kann. Das Terminal kommuniziert mit dem Terminal-Server über ein an einen asynchronen seriellen Anschluß (meist ein RS-232-Anschluß) angeschlossenes Modem. Das Terminal zeigt die Daten, die es vom Terminal-Server empfängt, nur an und führt keinerlei Weiterverarbeitung der Daten durch. Darüber hinaus wandelt das Terminal die Tastatureingaben des Benutzers in Daten um, die dann an den Terminal-Server gesendet werden.

Terminal-Server-Sitzung – Ende-zu-Ende-Verbindung zwischen einem Terminal und einem Terminal-Server. Die Terminal-Server-Sitzung beginnt im Normalfall, sobald der Ruf verbunden ist, und endet, wenn der Ruf beendet wird.

- Es gibt sowohl lokale als auch entfernte Terminal-Server-Sitzungen:

  Eine *lokale Terminal-Server-Sitzung* findet statt, wenn ein Terminal (oder ein Computer, der ein Terminal emuliert) mit dem „Control"-Anschluß der Ascend-Einheit verbunden ist bzw. wenn Sie von einem IP-Host aus eine Telnet-Verbindung zur Ascend-Einheit herstellen.

  In beiden Fällen starten Sie die Terminal-Server-Sitzung, indem Sie den Befehl „TermServ" aus dem Menü „Sys Diag" wählen und die Eingabetaste drücken. Lokalen Terminal-Server-Sitzungen steht nur ein Teil der Befehle zur Verfügung, auf die entfernte Terminal-Server-Sitzungen zurückgreifen können.

- Eine *entfernte Terminal-Server-Sitzung* findet über ein digitales Modem oder eine V.110- bzw. V.120-Verbindung zur MAX-Einheit statt.

  Ein *digitales Modem* ist ein Gerät, das über eine digitale Leitung (wie z. B. eine T1-PRI-Leitung) mit einem Modem an einer analogen Leitung kommunizieren kann. Wenn Sie über ein digitales Modem oder eine V.110- bzw. V.120-Verbindung auf einen Terminal-Server zugreifen, beginnt die entfernte Terminal-Server-Sitzung sofort. Der Befehl „TermServ" muß nicht extra gewählt werden.

Mit Hilfe eines integrierten digitalen Modems kann die MAX-Einheit eine entfernte Terminal-Server-Sitzung mit einer Datenübertragungsgeschwindigkeit von bis zu 28,8 KBit/s (ohne Datenkomprimierung) aufbauen. Die MAX-Einheit unterstützt alle gebräuchlichen Funktionen von Standard-Terminal-Servern, einschließlich Telnet, DNS (Domain Name Services), Anmeldungs- und Kennwortkontrolle, CDR- und Autorisierungsdiensten.

Thick Ethernet – Begriff, der einen Typ von Ethernet-Kabeln beschreibt und sich auf die relativ große Dicke der Koaxialkabel für Thick-Ethernet-Netzwerke bezieht (Durchmesser ca. 1 cm).

Thin Ethernet – Begriff, der einen Typ von Ethernet-Kabeln beschreibt und sich auf die relativ geringe Dicke der Koaxialkabel für Thin-Ethernet-Netzwerke bezieht (Durchmesser ca. 0,5 cm).

Tk-Anlage – *Telekommunikationsanlage*. Internes Telefonnetz, z. B. für größere Büros, bei der die ankommenden Rufe von einer gemeinsamen Nummer aus an verschiedene Nebenstellen und von einem Büro zum anderen weitergeleitet werden. Auch *Nebenstellenanlage* oder *PBX (Private Branch Exchange)* genannt.

Crossover-Kabel – Kabel, dessen Drähte sich kreuzen, so daß die Enden des Kabels jeweils die entgegengesetzte Anschlußbelegung aufweisen. Vergleiche „Geradeauskabel“.

UTP-Kabel – *Unshielded Twisted Pair Cable* (nicht abgeschirmtes Twisted-Pair-Kabel). Kabel, bei dem je zwei Aderpaare miteinander verdrillt sind, um die Rauschentwicklung zu unterdrücken.

gewählte Schaltung – Temporäre Verbindung zwischen zwei Endpunkten, die für die Dauer des Rufes aufgebaut wird und über die die beiden Seiten Daten austauschen können. Die Schaltung wird getrennt, wenn der Ruf beendet wird.

Videokonferenz – Kommunikation zwischen verschiedenen Standorten mit Bild und Sprache unter Zuhilfenahme eines digitalen Videoübertragungssystems. Digitale Videoübertragungssysteme bestehen im Normalfall aus Kamera, Codec, Netzzugangsgeräten, einem Netzwerk- und einem Audiosystem.

VT-100 – Von der Digital Equipment Corporation (DEC) hergestellter ASCI-Zeichen-Datenterminal, der aus einem Bildschirm und einer Tastatur besteht. VT-100 ist bei Datenterminals zum Industriestandard geworden. Mit Hilfe eines VT-100-Emulationsprogramms kann ein Standard-PC als VT-100-Terminal eingesetzt werden.

WAN – *Wide Area Network* (Fernnetz). Datennetzwerk, das häufig ein LAN über die Grenzen eines Gebäudes oder des Firmengeländes hinaus erweitert. WANs verwenden IXC- oder LEC-Leitungen, um eine Verbindung mit anderen LANs an anderen Standorten herzustellen. WANs werden im Normalfall mit Hilfe von *Bridges* oder *Routern* aufgebaut, um geographisch voneinander getrennte LANs miteinander zu verbinden.

Watchdog-Spoofing – dt. etwa: Watchdog-Überlistung. Wenn ein NetWare-Server keine Antwort auf die von ihm an einen Client gesendeten Watchdog-Sitzungs-*keepalive*-Pakete erhält, schließt dieser im Normalfall die Verbindung. Mit Watchdog-Spoofing antwortet die Ascend-Einheit jedoch im Namen der Clients

auf der anderen Seite der Brücke auf NCP-Watchdog-Anforderungen. Die Ascend-Einheit täuscht den Server-Watchdog-Prozeß also, indem sie ihm „vorgaukelt“, daß die Verbindung weiterhin aktiv ist.

Wide Area Network – Siehe „WAN“.

Zeichengabearten – Das sendende Gerät und das empfangende Gerät müssen Signale senden, um ihre internen Taktgeber (Uhren) zu synchronisieren und festzustellen, wo ein Datenblock aufhört und der nächste anfängt. Zur Aufrechterhaltung der Synchronisation und zur effektiven Übertragung von Daten verwendet die Leitung eine der beiden folgenden Zeichengabearten:

- Inband-Zeichengabe
- ISDN-D-Kanal-Zeichengabe

Siehe auch „Inband-Zeichengabe“ und „ISDN-D-Kanal-Zeichengabe“.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z